Office of the Secretary Of Defense (OSD)
Assistant Secretary of Defense (Research & Engineering)
11.3 Small Business Innovation Research (SBIR)
Proposal Submission Instructions

Introduction

The Assistant Secretary of Defense (Research & Engineering) SBIR Program is sponsoring topics in the Cyber-Physical Systems, Cognitive Readiness Personal Adaptive Training, Data Research, Energy and Power, and Information Assurance technology focus areas in this solicitation.

The Army, Air Force, and Navy are participating in the OSD SBIR Program on this solicitation. The service laboratories act as OSD's Agent in the management and execution of the contracts with small businesses. The service laboratories, often referred to as a DoD Component acting on behalf of the OSD, invite small businesses to submit proposals under the Small Business Innovation Research (SBIR) Program Solicitation.

In order to participate in the OSD SBIR Program, all potential proposers should register on the DoD SBIR Web site at http://www.dodsbir.net/submission as soon as possible. Follow the instructions for electronic submittal of proposals. It is required that all proposers submit their proposal electronically through the DoD SBIR/STTR Proposal Submission Web site at http://www.dodsbir.net/submission. If you experience problems submitting your proposal, call the SBIR/STTR Help Desk (toll free) at 1-866-724-7457.

Refer to Section 1.5 of the DoD Program Solicitation for the process of submitting questions on SBIR and Solicitation Topics. During the Pre-release period proposers have an opportunity to contact topic authors by telephone or e-mail to ask technical questions about specific solicitation topics, however, proposal evaluation is conducted only on the written proposal. Contact during the Pre-release period is considered informal, and will not be factored into the selection for award of contracts. Contact with the topic authors by telephone or e-mail subsequent to the Pre-release period is prohibited. To obtain answers to technical questions during the formal Solicitation period, please visit http://www.dodsbir.net/sitis. Refer to the front section of the solicitation for the exact dates

OSD WILL NOT accept any proposals that are not submitted through the on-line submission site. The submission site does not limit the overall file size for each electronic proposal; however, there is a **25-page limit**. File uploads may take a great deal of time depending on your file size and your internet server connection speed. If you wish to upload a very large file, it is highly recommended that you submit your proposal prior to the deadline submittal date, as the last day is heavily trafficked. You are responsible for performing a virus check on each technical proposal file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal.

Firms with strong research and development capabilities in science or engineering in any of the topic areas described in this section and with the ability to commercialize the results are encouraged to participate. Subject to availability of funds, the ASD(R&E) SBIR Program will support high quality research and development proposals of innovative concepts to solve the listed defense-related scientific or engineering problems, especially those concepts that also have high potential for commercialization in the private sector. Objectives of the ASD(R&E) SBIR Program include stimulating technological innovation, strengthening the role of small business in meeting DoD research and development needs, fostering and encouraging participation by minority and disadvantaged persons in technological innovation, and increasing the commercial application of DoD-supported research and development results. The guidelines presented in the solicitation incorporate and exploit the flexibility of the SBA Policy Directive to encourage proposals based on scientific and technical approaches most likely to yield results important to DoD and the private sector.

Proposal Submission

Refer to Sections 3.0 and 6.0 of the DoD Program Solicitation for program requirements and proposal submission. Proposals shall be submitted in response to a specific topic identified in the following topic description sections. The topics listed are the only topics for which proposals will be accepted. Scientific and technical information assistance may be requested by using the SBIR/STTR Interactive Technical Information System (SITIS). OSD's technical proposal page limit is 25 pages.

Description of the OSD SBIR Three Phase Program

Phase I is to determine, insofar as possible, the scientific or technical merit and feasibility of ideas submitted under the SBIR Program and will typically be one half-person year effort over a period not to exceed six months, with a dollar value up to $150,000. OSD plans to fund three Phase I contracts, on average, and down-select to one Phase II contract per topic. This is assuming that the proposals are sufficient in quality to fund this many. Proposals are evaluated using the Phase I evaluation criteria, in accordance with Section 4.2 of the DoD Program Solicitation. Proposals should concentrate on research and development which will significantly contribute to proving the scientific and technical feasibility of the proposed effort, the successful completion of which is a prerequisite for further DoD support in Phase II. The measure of Phase I success includes technical performance toward the topic objectives and evaluations of the extent to which Phase II results would have the potential to yield a product or process of continuing importance to DoD and the private sector, in accordance with Section 4.3 of the DoD Program Solicitation.

Subsequent Phase II awards will be made to firms on the basis of results from the Phase I effort and the scientific and technical merit of the Phase II proposal in addressing the goals and objectives described in the topic. Phase II awards will typically cover two to five person-years of effort over a period generally not to exceed 24 months (subject to negotiation), with a dollar value up to $1,000,000. Phase II is the principal research and development effort and is expected to produce a well defined deliverable prototype or process. A more comprehensive proposal will be required for Phase II.

For Phase II, no separate solicitation will be issued. Only firms awarded Phase I contracts, and that have successfully completed their Phase I efforts, may be invited to submit a Phase II proposal. Invitations to submit Phase II proposals will be released approximately at the end of the Phase I period of performance. The decision to invite a Phase II proposal will be made based upon the success of the Phase I contract to meet the technical goals of the topic, as well as the overall merit based upon the criteria in Section 4.3. DoD is not obligated to make any awards under Phase I, II, or III. For specifics regarding the evaluation and award of Phase I or II contracts, please read the front section of this solicitation very carefully. Phase II proposals will be reviewed for overall merit based upon the criteria in Section 4.3 of this solicitation.

Under Phase III, the DoD may award non-SBIR funded follow-on contracts for products or processes, which meet the Component mission needs. This solicitation is designed, in part, to encourage the conversion of federally sponsored research and development innovation into private sector applications. The small business is expected to use non-federal capital to pursue private sector applications of the research and development.

This solicitation is for Phase I proposals only. Any proposal submitted under prior SBIR solicitations will not be considered under this solicitation; however, offerors who were not awarded a contract in response to a particular topic under prior SBIR solicitations are free to update or modify and submit the same or modified proposal if it is responsive to any of the topics listed in this section.

Phase II Plus Program

The OSD SBIR Program has a Phase II Plus Program, which provides matching SBIR funds to expand an existing Phase II contract that attracts investment funds from a DoD acquisition program, a non-SBIR/non-STTR government program or Private sector investments. Phase II Plus allows for an existing Phase II OSD SBIR contract to be extended for up to one year per Phase II Plus application, to perform additional research and development. Phase II Plus matching funds will be provided on a one-for-one basis up to a maximum $500,000 of SBIR funds. All Phase II Plus awards are subject to acceptance, review, and selection of candidate projects, are subject to availability of funding, and successful negotiation and award of a Phase II Plus contract modification. The funds provided by the DoD acquisition program or a non-SBIR/non-STTR government program must be obligated on the OSD Phase II contract as a modification just prior to or concurrent with the OSD SBIR funds. Private sector funds must be deemed an “outside investor” which may include such entities as another company, or an investor. It does not include the owners or family members, or affiliates of the small business (13 CFR 121.103).

Fast Track Policy

The Fast Track provisions in Section 4.0 of this solicitation apply as follows. Under the Fast Track policy, SBIR projects that attract matching cash from an outside investor for their Phase II effort have an opportunity to receive interim funding between Phases I and II, to be evaluated for Phase II under an expedited process, and to be selected for Phase II award provided they meet or exceed the technical thresholds and have met their Phase I technical goals, as discussed Section 4.5. Under the Fast Track Program, a company submits a Fast Track application, including statement of work and cost estimate, within 120 to 180 days of the award of a Phase I contract (see the Fast Track Application Form on www.dodsbir.net/submission). Also submitted at this time is a commitment of third party funding for Phase II. Subsequently, the company must submit its Phase I Final Report and its Phase II proposal no later than 210 days after the effective date of Phase I, and must certify, within 45 days of being selected for Phase II award, that all matching funds have been transferred to the company. For projects that qualify for the Fast Track (as discussed in Section 4.5), DoD will evaluate the Phase II proposals in an expedited manner in accordance with the above criteria, and may select these proposals for Phase II award provided: (1) they meet or exceed selection criteria (a) and (b) above and (2) the project has substantially met its Phase I technical goals (and assuming budgetary and other programmatic factors are met, as discussed in Section 4.1). Fast Track proposals, having attracted matching cash from an outside investor, presumptively meet criterion (c). However, selection and award of a Fast Track proposal is not mandated and DoD retains the discretion not to select or fund any Fast Track proposal.

Follow-On Funding

In addition to supporting scientific and engineering research and development, another important goal of the program is conversion of DoD-supported research and development into commercial (both Defense and Private Sector) products. Proposers are encouraged to obtain a contingent commitment for follow-on funding prior to Phase II where it is felt that the research and development has commercialization potential in either a Defense system or the private sector. Proposers who feel that their research and development has the potential to meet Defense system objectives or private sector market needs are encouraged to obtain either non-SBIR DoD follow-on funding or non-federal follow-on funding, for

Phase III to pursue commercialization development. The commitment should be obtained during the course of Phase I performance, or early in the Phase II performance. This commitment may be contingent upon the DoD supported development meeting some specific technical objectives in Phase II which if met, would justify funding to pursue further development for commercial (either Defense related or private sector) purposes in Phase III. The recipient will be permitted to obtain commercial rights to any invention made in either Phase I or Phase II, subject to the patent policies stated elsewhere in this solicitation and awarded contract.

The following pages contain a summary of the technology focus areas, followed by the topics.

Cyber-Physical Systems Technology Focus Area:

The Department of Defense relies on many electro-mechanic devices with some sort of computer in them. These devices include aircraft, spacecraft, missiles, vehicles, ships, and increasing smaller things like rockets, rifles, and small robots. These devices are taking advantage of increasing computational power to increase the amount of automated control and to take on increasingly more complex tasks. Where the coupling of computational and physical domains is tight, these devices are known as Cyber-Physical Systems (CPS).

The topics written under this theme focus on:

1. Identifying *and* measuring the design, manufacturing, and operating principles of CPS that most affect system cost, performance, and development time.
2. Creating reference implementations (e.g., small ground robots or sensor control systems) that take advantage of basic research in CPS.
3. Objectively and verifiably demonstrating the improvements in system cost, performance, and development time of the reference implementations over similar systems which are not designed, manufactured, or operated with a disciplined and orderly understanding of CPS challenges.

The topic in this theme is:

OSD11-CP1	Enhancing Code Awareness in Software Development Environment

Cognitive Readiness Personal Adaptive Training Technology Focus Area:

The theme of the proposed efforts is to develop innovative methodologies/software/ hardware that will optimize an individual's ability to learn, experience, and retain knowledge. It is important to ensure that the lessons learned and knowledge retained prepares the individual for both their immediate mission and their career goals.

The training and learning environments should permit the course material to be automatically adaptable to incorporate the individual's cognitive strengths and weaknesses. This type of adaptable cognitive training would serve in a function similar to a personal trainer/coach. It would learn about an individual throughout their career and adapt course material in a manner best suited for the individual. This information could be stored on a microchip/Common Access Card (CAC)-type device and serves as an evolving personal adaptive trainer that makes the training more or less challenging depending upon the individual's measured performance. As an example, a pilot inserts the microchip into a flight simulator at the beginning of each session. The microchip adjusts the information presented in the simulator based on the pilot's previous and current performances in the simulator.

The critical efforts towards developing personal adaptive trainers include: 1) Content and data representation - The data must be digestible, trusted, and reusable within and across contexts in real time or long-term tracking, 2) Robust and unobtrusive monitoring of an individual's performance, including learning, fatigue, attention, and retention, 3) Diagnostic and predictive models for humans *and* agents - Model generation needs to be in real time and persistent. Models that require supercomputers for development and execution will not be feasible, 4) Real-time validation and verification tags to promote trust in the agents and their actions and assessments, and 5) Adaptive work and mission contexts – ability to tailor the environment in which the individual works so that the simulator and the working environment become one and the same.

The Cognitive Readiness Personal Adaptive Training Technology topics are:

OSD11-CR1	Adaptive, individualized training assessment capability (AITAC)
OSD11-CR2	Adaptive Desktop Trainer for ISR Imagery Analysis Based on Contextual Factors
OSD11-CR3	RPA Simulated Operational Communications and Coordination Integration for Aircrew Learning (SOCIAL)
OSD11-CR4	Integrated Adaptive SCORM, HLA and DIS Compliant Learning Content Management System

Data Research Technology Focus Area:

The Department of Defense is increasingly challenged by the amount of data available to analyze and assess threats in every area of operations and support of the military. In the information age the Department of Defense must counter traditional as well as asymmetric threats to national security. Current military operations will use both sensor data as well as new types of information openly available. Even more challenging is the identification of emerging threats, the definition of the features used to classify these new threats, along with the means of detecting these feature to ensure an appropriate and decisive military response.

Among the challenges within data analysis and use is the ability to overcome traditional sources of bias, for example sensor bias or sampling bias, within the data and the reuse or misuse of data and analysis for other than intended purposes. Sensor bias, for example, is impacted by the collection method which can lead to artificial impressions of network and activity shifts in systems over time. Sampling bias, as another example, can lead to an imbalance of coverage creating gaps overtime leading to risks of "undiscoverable nodes". The reuse of existing data sources expedites the data collection process but it also has the negative impact of potentially being incomplete and inconsistent, having structural gaps and limitations, or simply being old and no longer representative of the real world.

Research in the areas of mathematics, statistics, computational data analysis and visualization, computational sciences and computer science are of interest. In addition to the application of research methods and approaches, it is important to evaluate the impact of these efforts areas with regards to the way they change how data is collected, analyzed and assessed to meet a prescribed time for operational necessity and efficiency.

The Data Research Technology topics are:

OSD11-DR1	Contextual Sociocultural Reasoning in Weak Signal Environments
OSD11-DR2	Collaborative Visual Analytics Approach for Reasoning in Soft Information Fusion Domains
OSD11-DR3	Visual Representation and Implementation of Culturally Significant Information for Enhanced Tactical Decision-making
OSD11-DR4	Building Semantic Knowledge of Large Data Sets through Collaborative Visual Approaches
OSD11-DR5	Innovative approaches to Situation Modeling, Threat Modeling and Threat Prediction
OSD11-DR6	Discovering Valued Information in a Cloud Environment
OSD11-DR7	Video Data to DDMS Cards

Resilient Energy and Power Technology Focus Area

Engineering Resilient Systems is efficiently creating, fielding and evolving trusted defense systems that readily adapt to the inevitable changes in threat, technology, and mission environments in a wide range of contexts. Such systems are easily reconfigured or replaced for enhanced adaptability. Applying this concept to one of DoD's most crucial problems affecting future military systems, the development of advanced power systems, draws out the challenge to design and build power and energy systems with enough built-in resiliency to accommodate a wide range of dynamically changing mission scenarios, maximizing time on station (efficiency), firepower (peak power), or survivability as the system priorities change.

One area where both DoD and industry are lacking is in the area of cross domain tool development. Research & Development in this technology theme will provide a better scientific understanding and technical foundation for developing solutions the next generation of power systems synthesis tools. The majority of current tools are analysis tools, not synthesis tools – they target a specific domain and user group with significant delineations between models even within a single technology or analytical program; while access to cross domain tool sets linking multiple systems or holistically modeling single systems from cradle to grave, is limited.

The Resilient Energy and Power Technology topics are:

OSD11-EP1	Silicon Carbide Device Model Development for Circuit Simulations
OSD11-EP2	Human Machine Interface to Power and Energy Network

Information Assurance Technology in the Cyber Domain Focus Area

The cyber realm has emerged as a domain of battle where the DoD faces sophisticated and persistent adversaries pursuing strategic goals, rather than monetary gains or harassment. Even when no outward conflict is occurring, cyber adversaries may be exploiting our systems to gather information and position themselves for advantage in longer-term campaigns.

The DoD relies on commercial off-the-shelf (COTS) technology for cost-effective and rapidly advancing capabilities. However, COTS technology is equally available to aggressors to examine and prepare methods of attack on their own timetable. Further, the DoD does not control production of COTS hardware and software technology. Malicious elements could be inserted at any point in the supply chain of developers and manufacturers. Even security software can be undermined if it runs in a compromised environment. The situation is asymmetric. An attacker need only exploit a few flaws, while a defender must try to eliminate or counter them all. With relatively small resources, an adversary can create attacks marshalling large numbers of compromised components with damaging effect. The effort to safeguard and defend our systems and to find and clean up compromised components can be staggering.

The challenge for research in cyber operations and security is to develop techniques for operating successfully in this threatened cyber environment, and to reduce or reverse the asymmetry. Techniques, models, and tools are needed that allow cyber systems to accomplish their missions, with the assumption of partial compromise, though the attacks that inflicted it may have gone undetected. Networked systems must persevere, contain effects of incursions, blunt and frustrate attacks, and allow us to hunt and isolate adversaries within our networks, at Internet speeds.

Within this broad context, the following are areas of particular interest.

- Distributed trust: models and protocols for establishing, evaluating, and sustaining the appropriate level of trust among devices, components, or users in distributed interactions. These may include innovative authentication models and protocols, trust metrics and infrastructures, use of out-of-band context information, and trust maintenance protocols.
- Resilient architectures: architectural models and techniques that enable functional capabilities to continue despite disruption or compromise by an adversary. These may include techniques for unpredictability, dispersion, redundancy, and tolerance in systems processing and storage to make system tasks more difficult to target and disrupt.
- Visualization and decision support: analysis and presentation models and tools that enable human decision-makers to understand security and operational implications of cyber attacks and compromises, in view of both the immediate situation and prolonged cyber adversary campaigns, and to rapidly ascertain the best course of action to pursue.
- Response and cyber maneuver: techniques and tools that enable defenders to shape and minimize the attack space, frustrate adversary planning, and take action to block, disrupt, remove, or counter adversary actions. These may include techniques for polymorphism, obfuscation, network agility, and mission modeling.
- Military-grade hardware and protocols: hardened techniques and components for key system elements in situations where COTS is not sufficient, such as systems exposed to battlefield environments or those with cyber-physical effects.

Also of strong interest are techniques and tools for establishing and maintaining component trust, detecting and automatically responding to unanticipated methods of attack, and automatically recovering and reconstituting system capabilities and information context during and after attack.

The Information Assurance Technology in the Cyber Domain topics are:

OSD11-IA1	Anti-Exploitation Software Protection Systems
OSD11-IA2	Software Deception as a Countermeasure to Attacks on Software Protection Systems
OSD11-IA3	Identification of Critical Resources and Cyber Threats in the Physical Domain
OSD11-IA4	Cyber Security High Abstraction Contextual Visualization and Decision Support System
OSD11-IA5	Deterministic Detection for Hijacked Program Execution
OSD11-IA6	Active Software Defense to Reduce Threat Capability Effectiveness

OSD SBIR 11.3 Topic Index

OSD SBIR 11.3 Topic Descriptions

OSD11-CP1 TITLE: Enhancing Code Awareness in Software Development Environment

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: The objective to this solicitation is to develop techniques and methods for enhancing software robustness and security during development by enhancing software developers' understanding and awareness of their works, via automated capture and documentation of design decision (ACD3).

DESCRIPTION: Achieving information dominance requires Department of Defense (DoD) to maintain trust, availability and security within its information infrastructures. COTS based hardware and software in our computing systems and the network are large, complex and hence inherently insecure. Currently flaws in software are the major contributor to the vulnerability of cyber systems. Most if not all of these vulnerabilities originate from improper software implementations. Identified flaws that lead to improper implementations include, and are not limited to; buffer overflow, stack and heap overflow, dangling pointers, input data format violation, race conditions and deadlocks, etc. Significant investment has been made to address this issue through techniques that seek to provide formal or other forms of software verification. However, complementary efforts to verification, an automated method to enhance programmers awareness of his/her work during software development is under-explored.

Only rarely are all of the details for the implementation of software be specified in advance. Currently, programmers make instantaneous detailed design decisions during software coding. These instantaneous decisions (and assumptions) have far reaching effects, and they are often forgotten and lost. A tool that captures and documents these design decisions (and hence assumptions) automatically as coding is in progress can significantly enhance maintainability, robustness, and security of codes. The availability of these tools also presents an opportunity to provide feedback to programmers to improve the correctness of their product and enhance productivity and efficiency.

The objective to this solicitation is to develop techniques and methods for enhancing software robustness and security during development by enhancing software developers' understanding and awareness of their works and to develop a working prototype of a software development tool which performs automatic capture and document programmer's design decisions (ACD3), as coding is in progress. This software development tool should be applicable to one or more widely used programming languages, within common software development frameworks. The development of this tool may employ one or more of the following (partial) list of methods: capture and visualization of program structure and data, variable, and subroutine dependencies, capture of programmer's intent, analysis and prediction of consequences, formal analysis, etc. This solicitation does not entertain methods and tools specifically targeted for software verification.

PHASE I: Architectural analysis and design for the automated capture & documentation of design decision (ACD3) tool for an open-source software development environment of choice. Develop a proof of concept prototype for ACD3. Identify the metrics that determine the prototype's value-added.

PHASE II: Develop a full functioning prototype of a tool which performs automated capture & documentation of design decision (ACD3) for an open-source software development environment of choice. Demonstrate the efficacy for the tool.

PHASE III Dual Use Application: ACD3 is a valuable tool for both the DoD as well as for software developing public. It should find its role in, and can be ported into, various open-source and proprietary software development environments. ACD3 should also be applicable and portable to development environments of many different programming languages for many different application spaces, such as high performance computing, mobile devices, embedded systems, finance applications, cloud computing, the web and service oriented applications, etc.

REFERENCES:

1. Programmers Apprentice; http://csg.csail.mit.edu/CSGArchives/memos/Memo-231.pdf

2. Doxygen; http://www.stack.nl/~dimitri/doxygen/

3. Gradual Programming: Bridging the Semantic Gap;
http://www.cs.colorado.edu/~bec/papers/pldifit09-gradprog.pdf

4. "Program, Enhance Thyself!" – Demand-Driven Pattern-Oriented Program Enhancement
http://www.cs.vt.edu/~gback/papers/autoenhance-aosd2008.pdf

KEYWORDS: Software development environment, code quality, automated documentation, intent capture, on-the-fly formal analysis, real-time lint tool

OSD11-CR1 TITLE: Adaptive, individualized training assessment capability (AITAC)

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: The objective of this topic is to develop and implement a technique for building individualized representations of trainee performance that can be used to assess current performance and to forecast future training needs.

DESCRIPTION: Increasingly, instructional system developers are focusing their efforts on developing individualizable and adaptable training capabilities [1]. The benefits of providing this type of instruction are well documented [2] and are a direct result of the fact that individuals learn in different ways [3]. At the core of any adaptive training system are representations of the trainee, in terms of their knowledge, skills and abilities [4]. These representations are used by the instructional system to assess current trainee performance and to forecast the timing and content of future instructional remediations. A key challenge with building truly individualizable and adaptable training systems rests in the manner in which these trainee representations are developed. Typically, these representations are created using pre-defined performance measures, bounded by static parameters. Once a boundary is passed, a standard intervention is applied until the next iteration of performance assessment shows a return to within-parameter conditions.

The challenges with this approach are threefold. First, the set of performance measures used in a training system is often based on speed and accuracy characteristics. This approach precludes adding individual trainee-and training domain - unique measures, leading to a significant reduction in individualizability and adaptability. Second, the selected set of performance measures relies on establishing predefined thresholds to establish 'good' and 'poor' performance. This approach removes much of the richness and complexity of individual trainee performance, leading to inadequate timing, presentation and selection of training remediation. Lastly, because training systems base their anticipated training remediations on these static, average measurements, their future predictions of when trainees will need remediation, and what the content of that remediation should be, are inaccurate.

The current topic seeks to address these three challenges by developing and implementing a technique for building individualized representations of trainee performance that can be used to assess current performance and to forecast future training needs. The desired approach includes three elements. The first element includes developing a performance ontology that will: represent domain knowledge, reason about the elements and relations of that domain, support evaluation of performance and interpretation of data and provide scoring models and criteria for performance – to include cognitive, behavioral and physiological data [5]. The second element includes linking the resultant ontology to artificial intelligence or machine learning techniques to: dynamically make inferences and predictions about performance; and to handle uncertainty arising from latent variables or missing data [5]. The last element requires demonstrating the effectiveness of this capability to both accurately assess current trainee performance and to forecast future remediation requirements.

PHASE I: Define requirements for developing and implementing a technique for building individualized representations of trainee performance that can be used to assess current performance and to forecast future training needs. Requirements definition must include: a description of the overall ontology structure, the artificial intelligence technique that will be used and how the two will integrate; a determination of the types and characteristics of metrics that will be captured and used; a detailed discussion of the specific domain to be represented; and; and, a discussion of analysis and assessment techniques to be used. Phase II plans should also be provided, to include key component technological milestones and plans for testing and validation of the proposed system and its components. Phase I should also include the processing and submission of any necessary human subjects use protocols.

PHASE II: Develop a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include: (1.) a working prototype of the system, (2) specification for its development, and (3) demonstration and validation of ability to both accurately assess current trainee performance and to forecast future remediation requirements.

PHASE III: This technology will have broad application in military as well as commercial settings.
Within the military, there is increasing emphasis on the ability to develop training systems that tailor their instruction to individual trainee needs. Developing these 'cognitive tutors' is costly. Tools that will make building these systems more cost effective, as well as make the training more effective are needed. The proposed effort will enable the delivery of more effective training and will support knowledge sharing and reuse, leading to reduced up-front development costs. Commercially, the last several years has witnessed a resurgence in interest in developing individualized 'digital tutor' types of training systems for classroom (grades K-12) use (e.g. President Obama's 2011 State of the Union address), in support of Science, Technology, Engineering and Mathematics (STEM) education. The much wider range of learner characteristics of the K-12 student population can only be addressed by the types of technologies developed under this effort. Lastly, training in the commercial labor market is a multi-billion dollar business. Technologies that facilitate the application of adaptive training tools to a wide range of domains will lead to reduced cost and enhanced trainee learning experiences.

REFERENCES:

[1]. Fletcher, J.D. (2009). Education and Training Technology in the Military. Science 323:72-75.

[2]. Corbett, A, (2001). Cognitive Computer Tutors: Solving the Two-Sigma Problem. In M. Bauer, P.J. Gmytrasiewicz, and J. Vassileva (Eds.): UM 2001, LNAI 2109, pp. 137–147. Springer-Verlag Berlin Heidelberg.

[3]. Hawk, T.F. & Shah, A.J. (2007). Using Learning Style Instruments to Enhance Student Learning. Decision Sciences Journal of Innovative Education 5(1):1-19.

[4]. Cohn, J.V. (2009). Building Virtual Environment Training Systems for Success. In: D. Schmorrow, J. Cohn, & D. Nicholson (Eds.), PSI Handbook of Virtual Environments for Training and Education: Developments for the Military and Beyond. Santa Barbara, CA: Praeger Security International.

[5]. Koenig, A., Lee, J., Iseli, M., & Wainess, R. (2010). A Conceptual Framework for Assessing Performance in Games and Simulations. CRESST Report 771, http://www.cse.ucla.edu/products/reports/R771.pdf. Accessed on 08 April 2011.

KEYWORDS: Adaptive Training, Ontology, Machine Learning, Artificial Intelligence

OSD11-CR2 TITLE: Adaptive Desktop Trainer for ISR Imagery Analysis Based on Contextual Factors

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: Develop an adaptive desktop training device with underlying learning management system (LMS) architecture to train ISR imagery analysis for better decision making by warfighters.

DESCRIPTION: ISR imagery data has become paramount to military success in current operations in Iraq and Afghanistan. As more and more ISR platforms are being pushed into the operational environment it is becoming increasingly important to provide training that educates users on what they should expect to see from this imagery in the context that these assets will be deployed. Cultural, environmental, behavioral, economic, religious, and other factors play a significant role in the types of imagery users will observe in the AOR. Being aware of the context within a particular situation provides necessary information to determine if a potential target is for example: just filling in a hole as part of his/her job or covering up an IED. Additionally, understanding current and evolving tactics of insurgent operations are also an important factor in recognizing what is truly happening or about to happen in a situation and can mean the difference between life or death of troops and innocent civilians. A desktop training system is needed to train these users (Distributed Common Ground Station (DCGS) imagery analysts, Remotely Piloted Aircraft (RPA) crew members, ground troops who utilize ROVER feeds, etc) on how to interpret the actions they are seeing on the ground in order understand the significance of what is occurring and make better decisions about what actions to take. This system should provide an individually adaptive imagery training capability based on an underlying LMS architecture to bring users to a high degree of skill level to recognize events and situations on the ground using simulated Electro-Optical, Infrared, and Full Motion Video imagery. Furthermore, this system should have the ability to ingest new insurgent TTP information and other important factors (cultural, environmental, behavioral, economic, religious, etc) to adapt intelligent agent models and scenarios presented to users so that training can remain up-to-date with current operations. Finally, this system, though first developed as a standalone desktop environment, should have the capability for expansions into more complex operational simulation environments.

PHASE I: This phase will identify content for the development effort based on an assessment of operational needs. In addition, Phase I will develop a proof-of-concept desktop exemplar of the training and rehearsal concept to be fully developed in the Phase II effort.

PHASE II: Will build upon Phase I to fully develop, refine, test and evaluate the components of the system to include the underlying LMS, adaptive training course content, intelligent agent technologies and modular design for integration with an operational simulation environment. The final prototype will demonstrate these capabilities as well as the ability to ingest new or update material.

PHASE III DUAL-USE COMMERCIALIZATION:
Military Application: Imagery data for ISR is a major component of operations across all services. The developed technology would be beneficial for imagery analysts and warfighters who utilize IMINT sensors in DCGS, RPA, and ground operations.
Commercial Application: This training system would provide a beneficial tool for US Customs and Border Protection, homeland security, and natural disaster relief personnel who perform analysis on imagery data for decision making.

REFERENCES:

(1) DeGregorio, E.A., Messier, R.H., Shelton, J. and Castro, K. (2006). “Adapting Commercial Video Game Technology to Military Simulation Applications,” Australian SimTecT Conference.

(2) Carolan, T., Schurig, I. and Bennett, W. Jr. (2006). “Competency-based Training Adapting to Warfighter Needs,” (Technical Report No. AFRL-HE-AZ-TR-2006-0014). Mesa, AZ: Air Force Research Laboratory, Warfighter Readiness Research Division.

(3) Flynn, M., Pottinger, M., and Batchelor, P, “Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.” Center for a New American Security. January 2010. http://www.cnas.org/node/3924.

(4) Joint Publications Intelligence Series 2-0: (JP 2-0, Joint Intelligence; JP 2-01, Joint and National Intelligence Support to Military Operations; JP 2-03, Geospatial Intelligence Support to Joint Operations). Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jointpub_intelligence.htm

(5) Air Force Doctrine Document 2-9. “Intelligence, Surveillance, and Reconnaissance Operations” 17 July 2007. Retrieved from: http://www.e-publishing.af.mil/shared/media/epubs/AFDD2-0.pdf

(6) “Gateway to Intelligence” Air University Webpage. Retrieved from: http://www.au.af.mil/au/awc/awcgate/awc-ntel.htm

KEYWORDS: Imagery Analysis, Personalized Learning, Adaptive Training, Learning Management System, Desktop Training, Signal Detection, Imagery Intelligence Training

OSD11-CR3 TITLE: RPA Simulated Operational Communications and Coordination Integration for Aircrew Learning (SOCIAL)

TECHNOLOGY AREAS: Electronics, Human Systems

OBJECTIVE: The objective of this effort is to research, develop and implement prototype capabilities to simulate the communication and coordination of an operational Intelligence Surveillance and Reconnaissance environment for the purpose of providing: (a) Realistic RPA crew mission task saturation; (b) enhanced integration and coordination across an operational testbed environment; (c) a system to prototype, integrate and evaluate intelligent agents and synthetic teammates from both government and commercial sources at various levels of fidelity.

DESCRIPTION: In August 2010 operational Remotely Piloted Aircraft (RPA) crews visited AFRL Mesa to attend a training effectiveness workshop. During the workshop operators were asked for ideas to improve training. The consistent answer was to provide a capability for the RPA operators to interact and coordinate with other members of the ISR community (e.g. Mission Intelligence Coordinators) as they do in real world operations. Again in September 2010 during a follow up meeting with additional RPA crews, the same question was posed and the same answer was given. A system is needed that will create realistic task saturation in a simulated environment for ISR communication and coordination for improved training effectiveness for RPA operations and other command and control assets. This system should employ synthetic and intelligent agent technology to provide operationally realistic communication and coordination in the midst of a scenario but also have the capability to monitor individual performance and adapt the level of saturation to provide the appropriate level based on individual operator capabilities, essentially adaptive training for personalized learning. Additionally, the system should be designed to utilize existing operational community text based communication mediums (e.g. mIRC chat) to communicate. The modeled entities should be constructed synthetically and formatted so that both government and COTS systems may be used in parallel. The level of fidelity can interchangeably range from basic scripting to advanced intelligent architecture. The system should be capable of supporting multiple simulators for command and control training within an operational testbed.

PHASE I: Will research the operational needs, and result in the development of the initial underlying software architecture for this system and demonstrate its capabilities in a proof of concept to show functionality of each component of the total system.

PHASE II: Will fully develop the prototype software technology and underlying architecture and demonstrate the capability to provide task saturation and adapt the levels of saturation in an operational testbed in three different scenarios.

PHASE III DUAL-USE COMMERCIALIZATION:
Military Application: The military is increasingly relying more and more on chat communication for C2 operations. The development of this system would provide a capability that would apply to several domains and provide a new capability to improve operator ability to handle task saturation through personalized and adaptive training.
Commercial Application: This capability provides an adaptive training technology for task saturation for chat based communications in civilian contexts.

REFERENCES:

(1) Oikarinen, J., Reed, D., “Internet Relay Chat Protocol” Network Working Group, May 1993.

(2) Russell, S. J., Norvig, P., “Artificial Intelligence: A modern approach” Prentice Hall, 2010.

(3) Costello. M.B., “Flexible Soldier and Machine Interface for Micro Air Vehicles” Georgia Institute of Tech Atlanta School of Aerospace Engineering, 2006.

(4) Bailey, C., “Department of Defense Usage of FalconView” Georgia Tech Research Institute, 2007.

(5) Cantwell, H.R., “Operators of Air Force Unmanned Aircraft Systems Breaking Paradigms” Maxwell AFB, AL, AIR & SPACE POWER JOURNAL SUMMER, 2009.

(6) Daniel Gonzales et al., Network-Centric Operations Case Study: The Stryker Brigade Combat Team, Santa Monica, Calif.: RAND, MG-267-1-OSD, 2005.

KEYWORDS: Command and Control Training, Chat Communication Training, Task Saturation, Personalized Learning, Adaptive Training, Remotely Piloted Vehicle Training

OSD11-CR4 TITLE: Integrated Adaptive SCORM, HLA and DIS Compliant Learning Content Management System

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: Develop or modify existing Learning Management Systems (LMS) and Learning Content Management Systems (LCMS) to be able to use a Computerized Adaptive Testing (CAT) like process to adapt to a pre-established knowledge/skill baseline to dynamically alter SCORM, DIS, or HLA training content delivery

DESCRIPTION: Current military training is often linear and non-discriminatory. That is regardless of an individual’s base knowledge and skills the training content remains the same. This is especially true for DoD Computer Learning Content Information Management Systems (CLCIMS). In order to be effective in these times of high ops tempo with less and less opportunities for training, we need a training solution that is adaptive to an individual’s needs and can customize training to better prepare them for their mission and career. For this training solution to be a success at least four different components are required to interact with each another. 1) Develop or modify existing Learning Management Systems (LMS) to allow easy incorporation of ever changing essential competencies, skills, knowledge, and experience such as those defined in Air Force Mission Essential Tasks Lists (METLs), Training Task Lists (TTLs) or the Mission Essential Competencies (MEC) analysis to establish baseline skills and knowledge required for an individual to be successful in their mission/career rather than just training modules. 2) Develop a way to capture performance during training content delivery and mapping them to the establish baseline in the LMS. 3) Develop or modify existing Learning Content Management Systems (LCMS) to be SCORM, DIS, and HLA compliant. 4) Incorporate a Computerized Adaptive Testing (CAT) like process into the Learning Content Management System. Fully integrated we expect the LMS to track an individual’s performance mapped to an established baseline while the LCMS then dynamically adapt training scenarios/content based on the information stored in the LCMS. Additionally having the LCMS SCORM, DIS, and HLA compliant, content delivery can be in the form of Computer Based Training (CBT) or through a variety of Modeling and Simulation tools that utilizes DIS/HLA protocols depending on what training content/scenario is delivered. This allows training scenario/content to better fit the type of delivery to an appropriate learning environment. For the scope of this effort the targeted training audience will be the Senior Intelligence Duty Officer (SIDO) and Intelligence Duty Officer (IDO) of the Air and Space Operations Center (AOC). Their primary duties are Command and Control (C2) coordination as it relates to intelligence on the combat ops floor. However, the architecture in this training solution is ideally content-agnostic such that you can adapt the system for a multitude of military and civilian application.

PHASE I: Define and document the framework to easily incorporate new data sets such as knowledge, skills, and experiences into a LMS, identify how performance during content delivery is tracked and mapped to the LMS, to develop or modify existing LCMS to be SCORM, HLA, and DIS compliant, and define how to integrate a CAT like process into the LCMS. This includes identifying current LMS and LCMS and how they can be modified. Or if it is determined that a new LMS/LCMS is needed, define the approach.

PHASE II: Fully develop a proof of concept prototype to verify and demonstrate the four integrated component capabilities using the SIDO and IDO as usage cases. This includes the ability to add new data sets into the LMS, the ability for the LCMS to deliver SCORM, HLA, and DIS content, and the LCMS dynamically altering training content delivery based on performance tracking mapped to the baseline in the LMS.

PHASE III DUAL-USE COMMERCIALIZATION:
The proposed training solution is applicable to a variety of military and civilian applications. The immediate usage case is directly applicable to most individuals with C2 coordination as a primary duty on the military side such as those in Air Support Operations Centers (ASOC), Tactical Operation Centers (TOCs), Maritime Operation Centers (MOCs). On the civilian side these will include personnel assigned to homeland security or natural disaster relief C2 organizations at the county, state, or federal level. Additionally since the architecture is ideally content-agnostic, it can be modified for the Human Resources domain, education domain, etc.

REFERENCES:
(1) AFI 13-1AOCV1, Operational Procedures--Air and Space Operations Center. Available from www.e-publishing.af.mil

(2) Bersin, Josh; Howard, Chris; O'Leonard, Karen; Mallon, David (2009), Learning Management Systems 2009, Bersin & Associates

(3) Canterbury M. 1995. An Automated Approach to Distributed Interactive Simulation (DIS) Protocol Entity Development. Naval Postgraduate School. ADA305699. 127 p. Available from DTIC

(4) Colegrove, C. M. and Alliger, G. M. (2002). Mission Essential Competencies: Defining Combat Mission Readiness in a Novel Way. Paper presented at: NATO Research & Technology Organization, Studies, Analysis, and Simulation Panel, Conference on Mission Training via Distributed Simulation (SAS 38), Brussels, Belgium.

(5) Kamel M. 2007. Learning Management Systems: Practical Considerations for the Selection and Implementation of an E-learning Platform for the Navy. Naval Postgraduate School. ADA476768. 51p. Available from DTIC.

KEYWORDS: Learning Management System, Learning Content Management System, Computerized Adaptive Testing, SCORM, DIS, HLA, adaptive learning

OSD11-DR1 TITLE: Contextual Sociocultural Reasoning in Weak Signal Environments

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: Develop a method and implement a technique to correlate a variety of sociocultural, environmental, and geospatial data gathered from a region of interest to perform correlations and forecast likely future impacts of observations.

DESCRIPTION: Irregular warfare, non-state terrorism movements, and uncertain environmental patterns that trigger major weather disasters are producing a reality for military and government leaders where traditional physics-based sensors alone are insufficient to plan current and future actions in a region on interest or need. Context awareness is a critical requirement for decision makers because it provides important information about situations and dynamics relevant to goals, functions, and data needs [1]. Strategies for achieving contextual understanding can include observational data, a priori knowledge models, and inductive knowledge [2]. Contextual understanding is generally achieved through a combination of human and computer processing techniques that take advantage of a person's cognitive ability to fuse and assimilate multiple sources and types of information for new insights [3]. In the domains identified earlier in this topic, it is critical to incorporate both hard and soft data to gain an understanding of the delicate balance between individuals and groups in society and the environments (geopolitical, social, agricultural, etc.) upon which they depend. Test and evaluation of methods that fuse hard and soft data are challenging due to the nature of the data, the test environment, and the metrics for determining outcomes [4]. Unlike traditional military test and evaluation, however, data sources for this new type of problem are not classified or difficult to obtain; open source data is available and plentiful but it is collected by a diverse group of researchers. The challenge becomes correlating data of many different types that represent various aspects of a region of interest. This approach is similar to the signal processing approach of weak signal detection, that is used to extract received signals [5], identify images in noisy backgrounds [6], and conduct remote sensing of land and water resources for sustainable development of natural resources [7]. A novel approach to correlating a variety of data sources to understand problems in an area and forecast conflict is described by [8]. In this example, the potential conflict is the weak signal that is detected through the correlation of diverse datasets describing many features of the region, to include demographic, political, social, economic, educational, agricultural, weather, etc. A key challenge in integrating these disparate data is the semantic meaning implicit in the components of the overall structure of the region.

The challenges with this approach include the following. First, a method for collecting various datasets for a region of interest and correlating these for overall understanding and meaning is a nontrivial task. Many of the datasets are based on different scales and involve different referents to the population or the environment. Second, a weighting scale must be developed sufficient to provide representational meaning and inferential capabilities to the reasoning tool. Third, a visual representation must be developed sufficient for a human to reason about the correlations; a display that provides all of the facts but does not suggest inferences is insufficient and meaningless. Finally, a performance measurement capability is needed to compare the reasoning analytics to reasonable expectations for use of such a tool. Quantitative and qualitative metrics will be needed for such an application.

This topic seeks to address these challenges by developing and implementing a technique for correlating multiple datasets for a region of interest, weighting significant factors, and producing a set of forecasting alerts for a human user sufficient to trigger planning and course of action considerations.

PHASE I: Define requirements for developing and implementing a technique for building a technique that can be used to detect a ‘weak signal’ or troublesome behavior in a population or region of interest. Requirements definition must include: a description of the model components and the supporting relationships, the computational processing technique that will be used and a description of the integration mechanisms, a determination of the types and characteristics of the metrics that will be captured and used, a detailed discussion of the specific domain to be represented, and a discussion of analysis and assessment techniques to be used. Phase II plans should also be provided, to include key component technological milestones and plans for testing and validation of the proposed system and its components.

PHASE II: Produce a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include a working prototype of the system, specification for its development, and a demonstration and validation of the ability to both accurately represent the model of the soft information fusion and the collaborative visual analytics representation of the data.

PHASE III: This technology will have broad application in military, government, and commercial settings. Within the military and government, there is an increasing emphasis on understanding and forecasting group behaviors or regions that are prone to conflict or environmental degredation. Currently, fusing information from these multiple and divergent sources is extremely labor intensive and costly in terms of labor and time. Developing models that can forecast likely disruptions to fragile populations or environments will be a powerful addition to strategic, operational, and tactical decision making. The proposed effort will enable the delivery of more informed courses of action supported by tractable information sources in a display environment that provides multiple views into the problem space. Commercially, the advanced sensor technologies have produced unprecedented amount of digital information and applications by which to sort, collect, and share data. This sector has also witnessed a surge in analytic processing, dissemination, and display capabilities. Harnessing these for multiple uses will reduce the cost of integrating these techniques and improve the human decision making process.

REFERENCES:

[1] Rogova, G.L.; "Context-awareness in crisis management," Military Communications Conference, 2009. MILCOM 2009. IEEE , pp.1-7, 18-21 Oct. 2009.

[2] Gomez-Perez, J.M.; Moreno, C.R., "Overcoming Information Overload in the Enterprise: The Active Approach," Internet Computing, IEEE , vol.14, no.6, pp.39-46, Nov.-Dec. 2010.

[3] Secker, J.; Vachon, P.W., "Exploitation of multi-temporal SAR and EO satellite imagery for geospatial intelligence," Information Fusion, 2007 10th International Conference on, pp.1-8, 9-12 July 2007.

[4] Hall, D.L.; Graham, J.; More, L.D.; Rimland, J.C., "Test and evaluation of soft/hard information fusion systems: A test environment, methodology and initial data sets," Information Fusion (FUSION), 2010 13th Conference on, pp.1-7, 26-29 July 2010.

[5] Kang Lei; Mi Wujun; Lv Chao; Wang Shujuan, "Research on weak signal detection technique for electromagnetic ultrasonic inspection system," Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on, pp.2394-2399, 3-5 June 2008.

[6] Guangzhi Cao; Bouman, C.A.; Theiler, J., "Weak signal detection in hyperspectral imagery using sparse matrix transform (smt) covariance estimation," Hyperspectral Image and Signal Processing: Evolution in Remote Sensing, 2009. WHISPERS '09. First Workshop pp.1-4, 26-28 Aug. 2009.

[7] Rao, D.P., "A remote sensing-based integrated approach for sustainable development of land water resources," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol.31, no.2, pp.207-215, May 2001.

[8] West, K. “Scoping Out the Planet,” Scientific American. October 24, 2005. Available on the Internet at: http://www.scientificamerican.com/article.cfm?id=scoping-out-the-planet, downloaded June 4, 2011.

KEYWORDS: sociocultural terrain, weak signal detection, information fusion, correlation of diverse datasets, forecasting, fragile populations and environments.

OSD11-DR2 TITLE: Collaborative Visual Analytics Approach for Reasoning in Soft Information Fusion Domains

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop a method and implement a technique for using a collaborative visual analytics approach to the soft information fusion domain to enable humans to reason more efficiently in this complex information space.

DESCRIPTION: Increasingly, information fusion for strategic and tactical military decisions is driven less by the traditional physical domain and more by human or ‘soft’ sensor collectors and data products [1]. Recent trends in social networking and advanced computing have contributed to a significant change in the ways in which humans are represented in the information fusion domain; as targets and as sources of information [2]. As targets of the fusion system, individuals and groups, operating as open or hidden networks, are less tractable by physical sensors and the resulting behavior is difficult to infer and understand in advance of trigger events [3]. As information sources, human reports are subject to reporting bias, uncertainty, incompleteness, ambiguity, corruption, and perceptual/social bias [2, 6]. Finally, as decision makers, humans are distributed in time and space and require access to collaborative technologies to synchronize data, share information, and visualize potential courses of action [4]. In this extremely complicated space, understanding the data and manipulating the reasoning and display technologies through a user interface are basic starting points for more advanced capabilities [5]. The field of visual analytics has contributed tools to allow humans to solve analytical problems similar to those described above, albeit in a single user environment [7] or in a co-located team [8]. Collaborative Visual Analytics (CVA) is explored by [9], who describe an environment to allow remote-collaborative information exploration and task sharing with linked graphical interfaces. CVA has been used by an interdisciplinary team to predict the impact of global climate change on US power grids [10] and emergency response management [12]. The power of CVA for decision making in the soft information fusion domain stems from the inclusion of the social process of effort sharing, discussion, and consensus building [11] as well as the technical ability for team members to share representations, translate differing perspectives, articulate arguments, update conclusions, and justify actions [13].

The challenges with this topic are twofold. First, the soft information fusion domain is often described as 'data rich and model poor', which leads to the underlying need for a model that is flexible enough to incorporate disparate data and structured enough to support a decision maker's need to reason about the data. Second, collaborative visual analytics that can display information relationships and a team of users' individual reasoning requirements over those data artifacts is a complicated proposition and demands careful study and technical design.

The current topic seeks to address those challenges by developing and implementing a technique for building a collaborative visual analytics application for reasoning in a soft information fusion domain. The desired approach includes three elements. The first element includes developing a semantic model that can incorporate and parse elements of data into meaningful representations that are amenable to visual representation and manipulation. The second element is a performance evaluation and scoring mechanism by which a user community can be rated on ability to extract meaningful representations from the data. The last element requires demonstrating the effectiveness of this capability to model adaptations based on information inputs and also to assess user decision making as a function of the collaborative visual applications in a small team.

PHASE I: Define requirements for developing and implementing a technique for building a semantic model of soft information fusion that can be used in a collaborative visual analytics application for a small distributed team. Requirements definition must include: a description of the model components and the supporting relationships, the computational processing technique that will be used and a description of the integration mechanisms, a determination of the types and characteristics of the metrics that will be captured and used, a detailed discussion of the specific domain to be represented, and a discussion of analysis and assessment techniques to be used. Phase II plans should also be provided, to include key component technological milestones and plans for testing and validation of the proposed system and its components.

PHASE II: Produce a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include a working prototype of the system, specification for its development, and a demonstration and validation of the ability to both accurately represent the model of the soft information fusion and the collaborative visual analytics representation of the data.

PHASE III: This technology will have broad application in military, government, and commercial settings. Within the military and government, there is an increasing emphasis on understanding and forecasting group behaviors from social media and online social communities in foreign nations that are potentially hostile to US and Coalition interests. Currently, fusing information from these sources is extremely labor intensive and costly in terms of labor and time. Developing models that can be adaptive to new information and that can be utilized by a team of people with collaborative visual analytics reasoning tools will be a powerful addition to strategic, operational, and tactical decision making. The proposed effort will enable the delivery of more informed courses of action supported by tractable information sources in a display environment that provides multiple views into the problem space. Commercially, the online social blogs and social networking sites have produced unprecedented amount of digital information and applications by which to sort, collect, and share data. This sector has also witnessed a surge in analytic processing, dissemination, and display capabilities. Harnessing these for multiple uses will reduce the cost of integrating these techniques and improve the human decision making process.

REFERENCES:

[1] Hall, D.L.; McNeese, M.D.; Hellar, D.B.; Panulla, B.J.; Shumaker, W.; "A cyber infrastructure for evaluating the performance of human centered fusion," Information Fusion, 2009. FUSION '09. 12th International Conference on , pp.1257-1264, 6-9 July 2009.

[2] Hall, D. L., Jordan, J. M. Human-Centered Information Fusion. Boston: Artech House, 2010.

[3] Banerjee, P.K.; "Data fusion in defense and national security: Ubiquitous and indispensable," Circuits and Systems, 2007. MWSCAS 2007. 50th Midwest Symposium on, pp.762-765, 5-8 Aug. 2007.

[4] Blasch, E.; Hanselman, P.; "Information fusion for information superiority," National Aerospace and Electronics Conference, 2000. NAECON 2000. Proceedings of the IEEE 2000, pp.290-297, 2000.

[5] Posse, C.; White, A.; Beagley, N.; "Human-Centered Fusion Framework," Technologies for Homeland Security, 2007 IEEE Conference on, pp.111-116, 16-17 May 2007.

[6] Braun, J.J.; Glina, Y.; Hess, A.; Dasey, T.J.; Wack, E.C.; "Information fusion for CB defense applications: Challenge and opportunity," Technologies for Homeland Security, 2009. HST '09. IEEE Conference on pp.493-502, 11-12 May 2009.

[7] Isenberg, P.; Fisher, D.; Morris, M.R.; Inkpen, K.; Czerwinski, M.; "An exploratory study of co-located collaborative visual analytics around a tabletop display," Visual Analytics Science and Technology (VAST), 2010 IEEE Symposium on, pp.179-186, 25-26 Oct. 2010.

[8] Dong Hyun Jeong; Suma, E.; Butkiewicz, T.; Ribarsky, W.; Chang, R.; "A continuous analysis process between desktop and collaborative visual analytics environments," Visual Analytics Science and Technology (VAST), 2010 IEEE Symposium on, pp.231-232, 25-26 Oct. 2010.

[9] Keel, P.E.; "Collaborative Visual Analytics: Inferring from the Spatial Organization and Collaborative Use of Information," Visual Analytics Science And Technology, 2006 IEEE Symposium On, pp.137-144, Oct. 31, 2006-Nov. 2, 2006.

[10] Pak Chung Wong; Leung, L.R.; Ning Lu; Scott, M.J.; Mackey, P.; Foote, H.; Correia, J.; Taylor, Z.T.; Jianhua Xu; Unwin, S.D.; Sanfilippo, A.; "Designing a Collaborative Visual Analytics Tool for Social and Technological Change Prediction," Computer Graphics and Applications, IEEE , vol.29, no.5, pp.58-68, Sept.-Oct. 2009.

[11] Heer, J.; Agrawala, M.; "Design Considerations for Collaborative Visual Analytics," Visual Analytics Science and Technology, 2007. VAST 2007. IEEE Symposium, pp.171-178, Oct. 30 2007-Nov. 1 2007.

[12] Natarajan, S.; Ganz, A.; "Distributed visual analytics for collaborative emergency response management," Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE, pp.1714-1717, 3-6 Sept. 2009.

[13] Brennan, S.E.; Mueller, K.; Zelinsky, G.; Ramakrishnan, I.; Warren, D.S.; Kaufman, A.; "Toward a Multi-Analyst, Collaborative Framework for Visual Analytics," Visual Analytics Science And Technology, 2006 IEEE Symposium On, pp.129-136, Oct. 31 2006-Nov. 2 2006.

KEYWORDS: collaborative visual analytics, soft information fusion, decision making, reasoning, computer analytics, display techniques.

OSD11-DR3 TITLE: Visual Representation and Implementation of Culturally Significant Information for Enhanced Tactical Decision-making

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Using a visual analytics approach, develop a reasoning and display tool that will enable the visual representation and implementation of culturally significant information for enhanced tactical decision-making in a foreign and hostile environment.

DESCRIPTION: Modern warfare and conflict environments are drastically different from what was once considered to be the norm [8]. Where once the norm consisted of countryside “battlefield combat with distinct front lines,” modern conflict increasingly occurs in urban areas lacking distinct boundaries [8], within foreign cultures, where the focus is centered on the civilian population instead of the battlefield [1]. The discerning combatants from civilians has become increasingly complex in that combatants are frequently dispersed throughout the civilian population and without any clear uniform, it can be extremely difficult to discern friend from foe [8]. To further complicate combatant and civilian distinctions, a civilian encountered as such one day may present as a combatant another [8]. The conventional goal of overcoming an armed enemy is expanding, incorporating goodwill missions where the goal is to win over local civilians [8]. Operating in foreign environments, warfighters often find themselves in unfamiliar situations where they need to know how to resolve a situation appropriately in the context of an alien culture [4]. Due to these expansions in military conflict norms, sociocultural knowledge has become a critical factor for success in modern warfare environments [8]. Soldiers must understand a society's values, motivations, culture, and subcultures within in [1]. For mission success, it is critical for all Soldiers and commanders to maintain cultural situational awareness when in a foreign environment [1]. Effective situational awareness depends on the ability to collect data from many distributed, heterogeneous information-sources and through visual analytics, display the data so that it facilitates understanding of evolving events occurring within complex and dynamic environments [3]. The military has applied visualization techniques to enhance decision making [2]. Incorporating culturally significant information into a military database accessible by Soldiers and commanders will enhance decision-making.

The challenges with this topic are threefold. First, building and maintaining foreign cultural awareness and understanding societies where military operations are conducted has not always been a priority of the U.S. military [7]. It has been suggested that the lack of preliminary efforts to understand the local populace and culture that our forces operate in resulted in many of the early challenges encountered during Operations Iraqi Freedom and Enduring Freedom (OEF and OEF) [7]. Therefore, we are having back-track in order to develop and share cultural awareness while still immersed in these foreign cultures, and situations that have been exasperated by our lack of sociocultural awareness. Secondly, there are many challenges regarding data collection, entry, management, and quality. For instance, in regards to data entry, a large issue occurs with entity resolution and relationship awareness. How will a user discern two individuals with the same name? Answering these questions as well as exploring how to best visually represent this information to a user will be some challenges developers will confront. Regarding data quality, given that information may be coming from many different sources, data may overlap, be incomplete, or incorrect [5]. Determining how to overcome and compensate for these issues is an ongoing challenge for developers. Developers will have to determine how to fuse information collected from various types of data sources into meaningful information that will enhance human understanding without increasing user stress [3] and while compensating for any data errors [5].

The current topic seeks to address these challenges by developing and implementing a visual analytics technique for representing culturally significant information for enhanced tactical decision-making. This will include developing a semantic model that can incorporate and parse elements of data into meaningful representations that are amenable to visual representation and manipulation. Visual representations for sociocultural data that would prove critical for military operations regarding mission planning, hostile conflicts, and goodwill encounters. Visual and computer analytics should be employed to develop soft information and multi-source data fusion techniques. The tool should enable reasoning so that the sociocultural information could be applied to relevant mission scenarios such as route planning.

PHASE I: Define requirements for developing and implementing a technique for building a reasoning and display tool for enhanced visual representation of culturally significant information to promote commander decision making. Requirements definition must include: a description of the model components and the supporting relationships, the computational processing technique that will be used and a description of the integration mechanisms, a determination of the types and characteristics of the metrics that will be captured and used, a detailed discussion of the specific domain to be represented, and a discussion of analysis and assessment techniques to be used. Phase II plans should also be provided, to include key component technological milestones and plans for testing and validation of the proposed system and its components.

PHASE II: Produce a prototype system based on the preliminary design from Phase I. All appropriate engineering testing will be performed, and a critical design review will be performed to finalize the design. Phase II deliverables will include a working prototype of the system, specification for its development, and a demonstration and validation of the ability to both accurately represent the model of the soft information fusion and the collaborative visual analytics representation of the data.

PHASE III: This technology will have broad application in military, government, and commercial settings. Within the military and government, there is an increasing emphasis on understanding sociocultural norms and behaviors of communities in foreign nations that are potentially hostile to US and Coalition interests. Currently, fusing information from these sources is extremely labor intensive and costly in terms of labor and time. Developing collaborative visual analytics reasoning tools will be a powerful addition to strategic, operational, and tactical decision making. The proposed effort will enable the delivery of more informed courses of action supported by tractable information sources in a display environment that provides multiple views into the problem space. Commercially, the online social blogs and social networking sites have produced unprecedented amount of digital information and applications by which to sort, collect, and share data. This sector has also witnessed a surge in analytic processing, dissemination, and display capabilities. Harnessing these for multiple uses will reduce the cost of integrating these techniques and improve the human decision making process.

REFERENCES:

[1] Numrich, S.K.; "Culture, Models, and Games: Incorporating Warfare's Human Dimension," Intelligent Systems, IEEE, vol.23, no.4, pp.58-61, July-Aug. 2008. doi: 10.1109/MIS.2008.63

[2] Ten, D.W.H.; Manickam, S.; Ramadass, S.; Al Bazar, H.A.; "Study on Advanced Visualization Tools In Network Monitoring Platform," Computer Modeling and Simulation, 2009. EMS '09. Third UKSim European Symposium on, pp.445-449, 25-27 Nov. 2009. doi: 10.1109/EMS.2009.24

[3] Gilger, M.; "Addressing Information Display Weaknesses for Situational Awareness," Military Communications Conference, 2006. MILCOM 2006. IEEE , pp.1-7, 23-25 Oct. 2006. doi: 10.1109/MILCOM.2006.302129

[4] Zhou, H.; "Intelligent Cultural Advisor System: an interactive On-line Culture Guidebook," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, vol.1, pp.390-395, July 30 2007-Aug. 1 2007
doi: 10.1109/SNPD.2007.239

[5] Dawyndt, P.; Vancanneyt, M.; De Meyer, H.; Swings, J. "Knowledge accumulation and resolution of data inconsistencies during the integration of microbial information sources," Knowledge and Data Engineering, IEEE Transactions on, vol.17, no.8, pp. 1111- 1126, Aug. 2005. doi: 10.1109/TKDE.2005.131

[6] Altman Klein, Helen; Pongonis, Anna; Klein, Gary. “Cultural Barriers to Multinational C2 Decision Making,” 2000 Command and Control Research and Technology Symposium, 2000. Retrieved from: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA461631.

[7] Kipp, Jacob; Grau, Lester; Prinslow, Karl; Smith, Don. “The Human Terrain System: A CORDS for the 21st Century,” Military Review, Oct. 2006.

[8] Robert Pool, Rapporteur; Planning Committee on Unifying Social Frameworks; Board on Human-Systems Integration; Division of Behavior and Social Sciences and Education; National Research Council. (2011). Sociocultural Data to Accomplish Department of Defense Missions: Toward a Unified Social Framework. Washington, D.C.: The National Academies Press. Retrieved from: http://books.nap.edu/openbook.php?record_id=13077&page=R1.

KEYWORDS: culture, sociocultural awareness, visual analytics, soft information fusion, decision making, reasoning, computer analytics, display techniques.

OSD11-DR4 TITLE: Building Semantic Knowledge of Large Data Sets through Collaborative Visual Approaches

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Provide a technology application that builds semantic knowledge through metadata tagging capabilities and collaborative visual approaches, and includes multi-modal data feeds including text and visual data.

DESCRIPTION: Today’s information systems generate massive amounts of data and the areas of Defense and Homeland Security have the difficult task of quickly understanding and determining the crucial information from complex data systems [2,8]. Visual data mining and collaborative visual approaches to information can help handle the influx of information [6]. There is a corpus of data that, if sufficient data mining capabilities existed, could aid intelligence analysts in understanding information in near-real time [3]. A system that can extract information automatically from various multi-modal data sources and the efficient customization of a system to a new domain while defining a set of features and extraction rules are challenging tasks [1,7]. Many of the current folksomies do not control for spelling variations, synonyms, or clarification of homonyms. Controlled vocabularies such as a thesauri, classification schemes, and tools such as spell check or "text of 9 keys (T9)" could vastly reduce errors within reported data, improve search quality as well as enhance information discovery within a large database system [4]. Even if we could mine information via the tagged data, it is useless to users if it cannot be analyzed and employed in an operational setting [5]. These controlled tags should be easily accessible and users should be able to select and change appropriate tags at any time. An application with various user defined displays and layouts would be most useful in building semantic knowledge [2].

Challenges for this topic include 1) identifying relevant multi-modal data sets that incorporate various forms of text and visual data, 2) determine an effective tagging technique that can be used to increase accuracy of information systems, 3) develop a method to run the application with supporting tags in a pre-existing system, 4) demonstrate the ability to search and/or navigate the tagged database, 5) show the application's capability for visual analysis with various display options that can be utilized by distributed collaborative teams, 6) demonstrate the usefulness of this application in the broad realms of military, government, and commercial settings.

PHASE I: Develop a research plan that establishes the proof of concept for the application that will enable data tagging capabilities within a pre-existing large data set including text and visual data. Describe how the increased tagging abilities will support advanced searching and integrated visual analysis of various display options. Estimate the technical feasibility and value of the system and identify the essential technology issues that must be overcome to achieve success. Prepare a comprehensive research and development proposal for Phase II that includes critical plans for testing and evaluation of the system and its components.

PHASE II: Based on the preliminary plans of Phase I, produce a prototype application that is capable of enabling the tagging of various forms of data within an existing data set. The prototype should lead to a demonstration of the capability. Test the prototype in a large multi-sensor database including text and visual data to demonstrate the technical feasibility and merit of the product. Demonstrate a capability of enhanced data search capabilities that return relevant and related information for analysis that can be displayed in a variety of display options. Propose a verification and validation process.

PHASE III: Produce an application capable of deployment in an operational setting that can be utilized by distributed collaborative teams. Test the system in an operational setting as a component of a larger pre-existing multi-sensor database. The application should provide metrics for performance assessment. The work should focus on the ability to transition the tagging and searching system into the realm of military applications, other Federal Agencies, and/or private sector markets.

REFERENCES:

[1] Brandoli, B.; Eler, D.; Paulovich, F.; Minghim, R.; Batista, J.; "Visual Data Exploration to Feature Space Definition," Graphics, Patterns and Images (SIBGRAPI), 2010 23rd SIBGRAPI Conference on, pp.32-39, Aug. 30 2010-Sept. 3 2010 doi: 10.1109/SIBGRAPI.2010.13

[2] Decker, J.; Godwin, A.; Livingston, M.A.; Royle, D.; "A scalable architecture for visual data exploration," Visual Analytics Science and Technology, 2009. VAST 2009. IEEE Symposium on, pp.221-222, 12-13 Oct. 2009 doi: 10.1109/VAST.2009.5333451

[3] Drozdova, K. & Samoilov, M. (2009). Predictive analysis of concealed social network activities based on communication technology choices: Early-warning detection of attack signals from terrorist organizations. Computational Math Organizational Theory, DOI 10.1007/s10588-009-9058-2.

[4] Golub, K., Moon, J., Tudhope, D., Jones, C., Mathews, B., Puzon, B., & Nielsen, M.L. (2009). EnTag: Enhancing Social Tagging for Discovery. Joint Conference on Digital Libraries (JCDL), Austin, TX, June 15-19.

[5] Hak Lae Kim; Passant, A.; Breslin, J.G.; Scerri, S.; Decker, S.; "Review and Alignment of Tag Ontologies for Semantically-Linked Data in Collaborative Tagging Spaces," Semantic Computing, 2008 IEEE International Conference on, pp.315-322, 4-7 Aug. 2008. doi: 10.1109/ICSC.2008.79

[6] Keim, D.A.; "Information visualization and visual data mining," Visualization and Computer Graphics, IEEE Transactions on, vol.8, no.1, pp.1-8, Jan/Mar 2002 doi: 10.1109/2945.981847

[7] Phyu, A.L.L.; Thein, N.; "Domain Adaptive Information Extraction Using Link Grammar and WordNet," Creating, Connecting and Collaborating through Computing, 2007. C5 '07. The Fifth International Conference on, pp.47-53, 24-26 Jan. 2007 doi: 10.1109/C5.2007.11

[8] Rubel, O.; Prabhat; Kesheng Wu; Childs, H.; Meredith, J.; Geddes, C.G.R.; Cormier-Michel, E.; Ahern, S.; Weber, G.H.; Messmer, P.; Hagen, H.; Hamann, B.; Wes Bethel, E.; "High performance multivariate visual data exploration for extremely large data," High Performance Computing, Networking, Storage and Analysis, 2008. SC 2008. pp.1-12, 15-21 Nov. 2008 doi: 10.1109/SC.2008.5214436

KEYWORDS: data tagging, decision support, intelligence analysis, multi-sensor data fusion, information extraction

OSD11-DR5 TITLE: Innovative approaches to Situation Modeling, Threat Modeling and Threat Prediction

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Innovative approaches to Situation Modeling, Threat Modeling and Threat Prediction for improved Situational Awareness.

DESCRIPTION: The Joint Directors of Laboratories (JDL) Subpanel on Data Fusion has defined Data Fusion as "a process dealing with the association, correlation, and combination of data and information from single and multiple sources to achieve refined position and identity estimates, and complete and timely assessments of situations and threats, and their significance. The process is characterized by continuous refinements of its estimates and assessments, and the evaluation of the need for additional sources, or modification of the process itself, to achieve improved results".

Steinberg, et al [Reference 1] later defined data fusion as "the process of combining data to refine state estimates and predictions." A breakout of the functional levels [1] is:

- Level 0 - Sub-Object Data Assessment: estimation and prediction of signal/object observable states on the basis of pixel/signal level data association and characterization;
- Level 1 - Object Assessment: estimation and prediction of entity states on the basis of observation-to-track association, continuous state estimation (e.g. kinematics) and discrete state estimation (e.g. target type and ID);
- Level 2 - Situation Assessment: estimation and prediction of relations among entities, to include force structure and cross force relations, communications and perceptual influences, physical context, etc.;
- Level 3 - Impact Assessment: estimation and prediction of effects on situations of planned or estimated/predicted actions by the participants; to include interactions between action plans of multiple players (e.g. assessing susceptibilities and vulnerabilities to estimated/predicted threat actions given one's own planned actions);
- Level 4 - Process Refinement (an element of Resource Management): adaptive data acquisition and processing to support mission objectives.

To date the majority of data fusion research, development, and applications focus primarily on the lowest levels of data fusion (e.g., Level 1 – Object Refinement). The higher levels of information fusion (HLF) are inadequately being addressed, in particular the areas of Situation Modeling, Threat Modeling, and Threat Prediction. This SBIR effort will therefore address these three domains, taking into account bias, uncertainty, and ambiguity within the data.

The specific area of research to be addressed for this topic is: research, development and application of novel methods to model and characterize the quality of data when it is reused for alternative purposes. This includes estimating the uncertainty or error in the resulting analysis due to the alternative data usage. The data that are available for reuse could include a mixture of quantitative/qualitative data types and are from structured and unstructured repositories or sources.

Impact: One could understand what is missing in the data and fill in the gaps by gaining a better understanding of how and why the original data were collected. Of particular interest are situations where data are gathered across different domains (physical, non-physical, cyber, medical, etc.) and are subsequently used for analysis in another domain.

PHASE I: The proposal for Phase I should identify an innovative approach for improving situational awareness through the use of novel methods to model and characterize the quality of data when it is reused for alternative purposes. This includes estimating the uncertainty or error in the resulting analysis due to the alternative data usage. The data that are available for reuse could include a mixture of quantitative/qualitative data types and are from structured and unstructured repositories or sources. The study should provide a detailed discussion on uncertain, incomplete and ambiguous data/information and how it is used in the Higher Level Fusion process.

PHASE II: In Phase II, development of a prototype Higher Level Information Fusion system based on the Phase I design. Demonstrate the developed Higher Level Information Fusion prototype to prove feasibility for improving situational awareness by novel methods to model and characterize the quality of data when it is reused for alternative purposes through the development of novel methods to model and characterize the quality of data when it is reused for alternative purposes.

PHASE III Dual Use Applications: There are many dual use applications of Information Fusion techniques. For example in the law enforcement community, this research could be applied to counter narcotics arena or Homeland Defense. On the commercial side, this research is applicable to business intelligence, where companies attempt to determine what their competitors are doing by collecting and analyzing data available over the web.

REFERENCES:

1. A. Steinberg, C. Bowman, F. White, "Revisions to the JDL Data Fusion Model", Proc. Of the SPIE Sensor Fusion: Architectures, Algorithms, and Applications III, pp 430-441, 1999.

2. E. Waltz and J. Llinas, "Multisensor Data Fusion", Artech House, 1990.

3. R. Antony, "Principles of Data Fusion Automation", Artech House, 1995.

4. M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems”, Human Factors Journal, 37(1), pages 32-64, March 1995.

5. E. Bosse, J. Roy, S. Wark, “Concepts, Models and Tools for Information Fusion, Artech House, 2007.

KEYWORDS: Information Fusion, Higher Level Fusion, Data Fusion, Knowledge Discovery, Situation Assessment, Threat Assessment, Impact Assessment; Situation Modeling; Threat Modeling; Threat Prediction, Data Reuse, Data Analysis, Sensor Bias.

OSD11-DR6 TITLE: Discovering Valued Information in a Cloud Environment

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Design and implement a populated architecture that can quickly and efficiently discover actionable tactical information contained or derived from large parallel data stores. A user friendly interface should be able to translate a condition of interest into a parallelized map reduce job. The system should also be able to recognize redundancies in data held within large parallel data stores to prevent sparse evidence from being viewed as a well supported inference. The mature system should provide a common data currency for exchange across a large parallel enterprise through use of data dictionaries, shared ontologies and maps to data sources. A request for unusual events must be understand in the context of many types of data and many different types of mission information requirements. All data and services should be discoverable by a tactical user equipped with only a PDA.

DESCRIPTION: In combating terrorism the need exists to monitor at risk individuals and groups. The data sources to achieve this goal can consist of military sensors and sources as well as open source literature. Key data types that may contain valued information include unstructured text, audio files, images, high resolution imagery, wide area airborne imagery and biometric data Currently, there does not exist a way to run specific searches in response to a tactical information need against large distributed data stores. Sensor data can be 1) stored in a large data archive for retrieval and extraction, 2) kept at an aggregation node (gateway), or 3) remain close to smart sensor and triggers provided for data distribution. The goal of the topic is to mature a set of map reduce tools that can address key warfighter questions quickly by fusing interim results obtained by running code in parallel across numerous multi-INT data stores. Map reduce jobs must be configured and activated by an easy to use tactical PDA based user interface that understands the language commonly used to express priority and specific information requirements. After a single knowledge product is produced from the combination of many work tasks applied across many data stores, that product must be delivered to the warfighter. The matured system must be able to produce answers in real time. For this topic, offerors may work with the following distributed data sources; warfighter observations containing time/location stamps and unstructured text, images with time/location stamps and unstructured text comments; and biometric reports containing time/location stamps. Phase 1 performers may work with synthetic data. The Hadoop framework should be utilized. The offeror should work towards a capability to allow a warfighter to ask for activity reports relevant to a location over a specified time and receive a summary derived from the content of distributed data stores. The specific challenges of this topic include: 1) Maturing a set of related map reduce jobs that can act on distributed stored images/imagery, unstructured text and biometrics data to find data that relates to a priority or specific information requirement 2) Development of a level one fusion engine based on FrameNet that can combine the output of a number of map reduce jobs run against a distributed data store to produce a single knowledge product 3) Development of a user GUI that allows the warfighter to input a time/space bounded information requirements and be returned successfully mined information 4) development of semantic search map reduce jobs and a PDA triggered workflow manager.

Research in the areas of mathematics, statistics, computational data analysis and visualization, computational sciences and computer science are of interest. In addition to the application of research methods and approaches, it is important to evaluate the impact of these efforts areas with regards to the way they change how data is collected, analyzed and assessed to meet a prescribed time for operational necessity and efficiency. It is of value to use open standards to reduce costs [4].

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a plan and detailed approach for populating an architecture that can address warfighter questions by simultaneously processing multi-INT distributed data stores. Identify the critical technology issues that must be overcome to achieve success. Technical work should focus on the reduction of key risk areas. For a constrained set of warfighter questions and distributed data stores, demonstrate that phase 1 risk reduction work has shown that a full implementation of the approach is technically tractable. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Produce a prototype system that is capable of distributed processing in a cloud environment. The prototype system should assemble information by automated means, provide performance metrics and offer visualization appropriate to user’s device. Produce a prototype distributed processing service that can produce accurate answers to warfighter questions by simultaneously processing large distributed varied data sources. The prototype should enable a demonstration of the capability to be conducted using relevant data sources, some of which may be classified. The prototype should be capable of operating in a real time mode. Identify appropriate test performance dependent variables and make trade-off studies. Address bias in data processing due to redundant sampling. The prototype should be relevant to both DoD and commercial use cases.

PHASE III: Produce a system capable of deployment in an operational setting. The work should focus on a specific user environment intended for product transition. Test the system in an operational setting in a stand-alone mode or as a component of shared processing environment. The work should work towards a transition to program of record, military organization or commercial product. The system should adhere to open standards and use registered COI vocabulary and ontologies where feasible.

REFERENCES:
1. Apache Software Foundation. ActiveMQ. 9/22/2010 http://activemq.apache.org

2. Apache Hadoop: http://hadoop.apache.org/

3. FrameNet: http://framenet.icsi.berkeley.edu/

4. Cloud computing, wikipedia 2011, http://en.wikipedia.org/wiki/Cloud_computing

5. Open Networking Foundtion formed to Speed Network Innovation, March 21, 2011
http://www.openflow.org/wp/2011/03/open-networking-foundation-formed-to-speed-network-innovation/

KEYWORDS: cloud computing, data dictionaries, ontology, data sharing, data fusion, map reduce

OSD11-DR7 TITLE: Video Data to DDMS Cards

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Design and system that can automatically generate a stream of metadata cards consistent with the DoD Discovery Metadata Specification (DDMS). Currently the dissemination of video data requires that a human isolates and annotates specific frames. Metadata cards that are exposed to DoD ISR enterprise contain little more that the coordinates of the area that was imaged and the time markers for the first and last frame. Semantic searches on large video holdings cannot currently be done. This topic seeks to support technology maturation as needed to enable real time and forensic semantic searches on video data.

DESCRIPTION: In combating terrorism the need exists to better exploit video data in real time for force protection and mission execution. In recent years, major advancements in video analytics have enabled object and selected rule based behavior recognition, but connecting the expressions used in describing these detections semantically to priority and specific intelligence requirements has lagged. The specific challenges of this topic include:
1) Authoring a mapping of typical tactical warfightr priority and specific intelligence requirements to the possible output of video analytic engines 2) Development DDMS compliant real time video analytic engines 3) Expansion of the DDMS specification as needed to better capture the semantics of video understanding and mission intelligence requirements 4) Focusing and expansion of video analytic capabilities to be more responsive to priority and specific tactical intelligence requirements 5) Development of a user GUI that allows the warfighter to input priority and specific information requirements and map those questions into standing DDMS compliant metadata card searches 6) development of the overall system architecture that enables the workflow described above 7) development of visualization technology that allows the warfighter to quickly understand the significance of returned data to his/her set of information requirements.

Research in the areas of mathematics, statistics, computational data analysis and visualization, computational sciences and computer science are of interest. In addition to the application of research methods and approaches, it is important to evaluate the impact of these efforts areas with regards to the way they change how data is collected, analyzed and assessed to meet a prescribed time for operational necessity and efficiency. It is of value to use open standards to reduce costs.

The OSD is interested in innovative R&D that involves technical risk. Proposed work should have technical and scientific merit. Creative solutions are encouraged.

PHASE I: Complete a plan and detailed approach for populating an architecture that enables video processors to automatically publish metadata cards that are compliant to the DDMS specification and responsive to tactical priority and specific intelligence requirements. Identify the critical technology issues that must be overcome to achieve success. Technical work should focus on the reduction of key risk areas. For a constrained set of warfighter priority and specific intelligence requirements and a constrained set of entities and behaviors of interest, demonstrate that phase 1 risk reduction work has shown that a full implementation of the approach is technically tractable. Prepare a revised research plan for Phase 2 that addresses critical issues.

PHASE II: Produce a prototype system that is capable of translating full motion video into a set of DDMS compliant semantic meta data cards that can be automatically connected to subscribed to priority and specific intelligence requirements. The prototype system should run at the sensor and fully connect to the DoD ISR enterprise and command and control programs of record. Produce a prototype distributed processing service that can automatically deliver the right video clip to the right warfighter by simultaneously tagging video and understanding information subscriptions. The prototype should enable a demonstration of the capability to be conducted using relevant data sources, some of which may be classified. The prototype should be capable of operating in a real time mode. The prototype should be relevant to both DoD and commercial use cases.

PHASE III: Produce a system capable of deployment in an operational setting. The work should focus on a specific user environment intended for product transition. Test the system in an operational setting in a stand-alone mode or as a component of shared processing environment. The work should work towards a transition to program of record, military organization or commercial product. The system should adhere to open standards and use registered COI vocabulary and ontologies where feasible.

REFERENCES:

1. DDMS: http://en.wikipedia.org/wiki/Defense_Discovery_Metadata_Specification

2. Priority Intelligence Requirements: http://www.fas.org/irp/doddir/army/fm34-2/Appd.htm

3. Video Analytics: http://en.wikipedia.org/wiki/Video_Content_Analysis

KEYWORDS: DDMS, metadata, video analytics, intelligence requirements, alerting

OSD11-EP1 TITLE: Silicon Carbide Device Model Development for Circuit Simulations

TECHNOLOGY AREAS: Ground/Sea Vehicles, Electronics

ACQUISITION PROGRAM: PEO CS&CSS

OBJECTIVE: The development of fast SiC device models for high level circuit-design packages such as, for example, Pspice and Sabre.

DESCRIPTION: The military has been developing advanced high-power wide bandgap semiconductor electronic devices, especially in silicon carbide (SiC), for improved efficiency and high-temperature (100 to 200 ºC) operation. SiC Schottky diodes are beginning to be broadly incorporated into power electronic systems, with the expectation that SiC-based power switches (such as MOSFETs and JFETs) will soon follow. Design of efficient SiC-based power systems requires a detailed understanding of the circuit operation of SiC power devices. Compact circuit models with a high degree of accuracy, yet portable, are critical to the design process and require fast device models.

Much work has gone into developing device models to accurately predict performance of individual devices and such devices are now commercially available. There is a need to develop the next level of models to provide circuit designers the ability to evaluate circuits that utilize these devices such as been done for silicon-based electronic packages. These models will need to take into account the multi-disciplinary modeling requirements to accurately predict how the devices will function in circuits. The models should address electrical, thermal, mechanical, and material calculations while providing the designer accurate results in steady state, time, and frequency domains.

Particular challenges include the development of high-speed models appropriate for circuit level design while maintaining the accuracy of models based on first principles from device physics, thermodynamics, heat transfer, mechanics, and material science.

PHASE I: Provide initial innovative device modeling that can enable the reliable design of SiC power circuits. Demonstrate the feasibility of expanding the initial modeling concept to all design criteria desired in the above description. All models should be scalable and of flexible use for multiple applications.

PHASE II: Develop and mature the model from Phase I to include electrical, thermal, mechanical, and material calculations. The model's reliability should be demonstrated on at least two independent SiC circuits of differing utility while providing accurate results in steady state, time, and frequency domains.

PHASE III: Further expand the utility of the model under varying circuit design and conditions while enhancing portability. Undergo more rigorous test and evaluation on a greater variety of circuits.

REFERENCES:
1. J.B. Cassady and R.W. Johnson, Solid State Electronics, vol. 39, pp. 1409-1422 (1996).

2. S. Potbhare, N. Goldsman, A. Akturk, A. Lelis, Materials Science Forum, vols. 645-648, pp. 1163-1166 (2010).

3. T.R. McNutt, A.R. Hefner, Jr., H.A. Mantooth, D. Berning, and S-H Ryu, IEEE Transactions on Power Electronics, vol. 22, pp. 353-363 (2007).

4. S. Potbhare, N. Goldsman, A. Lelis, J.M. McGarrity, F.B. McLean, and D. Habersat, IEEE Transactions on Electron Devices, vol. 55, pp. 2029-2040 (2008).

KEYWORDS: Circuit Models, Electronic Package Design, Silicon Carbide

OSD11-EP2 TITLE: Human Machine Interface to Power and Energy Network

TECHNOLOGY AREAS: Ground/Sea Vehicles, Electronics

ACQUISITION PROGRAM: PEO CS&CSS

OBJECTIVE: To develop a semi-autonomous operator's control center for operational power and energy networks in military systems.

DESCRIPTION: The military has been developing advanced Power and Energy Networks that will allow for more efficient, flexible, and resilient energy security systems. There is a need to develop the human-machine interface enabling the operator to control and influence the network, ensuring the network is achieving its optimal potential in relevant operational environments. The interface would need to display the state of the system and all components that make up the power and energy network as well as allow for controlling that state, including alerts of power spikes or drains, thermal issues, electrical parameters and discontinuities, and mechanical health. The interface will display recommendations for steps the operator may undertake to mitigate any problems, ranging from additional focused monitoring to manual emergency shut-down.

Challenges include the development and integration of appropriate models that represent the power and energy system and obtaining accurate sensor information from constituent devices. Further challenges are displaying the information in an understandable format and allowing for an efficient response time for the operator interaction with the network's mechanics.

PHASE I: Catalogue and report the current state of the art cognitive visualization models. To be included is the human factor engineering specifications of utilizing the visual space and design for optimizing understanding of the network state. Care should be directed to determining when the network state goes beyond specific metrics requiring human interruption to restore normalcy with suggested actionable options. Catalogue and report the current state of the art of autonomous technology for power and energy networks and controls. Report the possible integration points of combining the two areas into a system that would allow for semi-autonomous control of a power and energy system.

PHASE II: Identify the technical gaps from merging the cognitive visualization with the autonomous tools that engage the user and allow for understanding at an unburdened state. Begin the process of modeling, prioritizing and solving the gaps to create a system that is adaptable and robust to meet any unanticipated, emergent phenomenon. Begin preliminary design of system architecture and hardware for the automated control of simple and complex power network, with human-machine information exchange displays and interaction.

PHASE III: Further expand the utility of the model and the interaction hardware for display and controls. Undergo more rigorous test and evaluation on complex networks likened to large Forward Operating Base, Remote-Austere Airfields, Electric Ships, and vehicles.

REFERENCES:

1. S. Clark, J. Steventon, and R. Masiello, "Full-Graphics Man-Machine Interface for Power System Control Centers", IEEE Paper # 0895-0156/88/0700-0027, 1988.

2. http://www.integraxor.com/

3. http://www.epiphan.com/

4. http://www.powereng.com/projects/index.aspx?id=385

5. http://www.massgroup.com/solutions/automotiveSCADAHMI.asp

6. L. Réveilleau, E. Becquet, L. Bacon, J-M. Douin, E. Gressier-Soudan, F. Horn, "Towards a RT-Java Based Embedded Remote Monitoring Tool for Small and Medium Power Plant Units".

7. H. Amelink, A. Hoffmannau, E. Becquet, L. Bacon, J-M. Douin, E. Gressier-Soudan, F. Horn, "Current trends in control centre design", International Journal of Electrical Power & Energy Systems, Volume 5, Issue 4, October 1983, Pages 205-211

8. Q. Zhijian, L Mingguang, L. Li, H. Zhiqing, Y. Gang, "UML Design of Power Automation Human Machine Interface System Based on SVG and AJAX," Intelligent Systems and Applications, 1-4 (2009).

9. Y. L. Murphey, M. A. Masrur, and D. E. Neumann, "Exploring Cognitive Knowledge for Intelligent Vehicle Power Management in Military Mission Scenarios", NDIA publication.

10. J. Park, Z. Chen, L. Kiliaris, M. Kuang, M. Masrur, A. Phillips, Y. Murphey, "Intelligent Vehicle Power Control Based on Machine Learning of Optimal Control Parameters and Prediction of Road Type and Traffic Congestion", IEEE Transactions on Vehicular Technology, Nov. 2009, Volume: 58 Issue:9, pp. 4741 - 4756

11. R. Beach, G. Kimnach, T. Jett, L. Trash, "Evaluation of power control concepts using the PMAD systems test bed", IECEC-89., Proceedings of the 24th Intersociety Issue Date: 6-11 Aug 1989.

KEYWORDS: Power, electrical power, Human-Machine Interface

OSD11-IA1 TITLE: Anti-Exploitation Software Protection Systems

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop software protection systems that are difficult to exploit once an adversary gains entry.

DESCRIPTION: State-of-the-art software protection and anti-tamper systems are built based upon three basic tenets: (1) reduce system susceptibilities, (2) move critical information out-of-band to the attacker, and (2) reduce the effectiveness of our adversaries' capabilities through detection, response and adaptive mechanisms [1]. For the most part, however, computer, sensor, and weapons systems are built using untrusted commercial-off-the-shelf (COTS) parts. Supply chain threats to critical components, such as hardware or firmware Trojans, have invalidated the assumption that we can move our critical software and data "out-of-band" to the adversary, such as in a hypervisor or on "secure" hardware, since the hardware components on which the software ultimately executes is untrusted [2]. Detection techniques currently being researched to address this class of threat, while important and useful, only reduce the likelihood of exploitation, not eliminate it; and it is only a matter of time before those measures fail. In short, the concept of keeping an adversary outside of a protected volume, layer, or device has been completely eroded by supply chain threats. As a result, one must take a long-term strategic view and assume in designing protection systems that an unknown subset of the system on which that software executes (e.g., an integrated circuit, printed circuit board, or subsystem) will eventually be compromised.

While novel techniques have been proposed for mitigating low-level persistent threats, such as firmware and hardware Trojans in COTS hard disk drives and other peripherals in desktop systems, the typical attack surface of a computer or weapon system is so large that these approaches and concepts, even if successfully applied to these devices, will not scale to protect the entire system. One must, therefore, re-think the fundamental approach to building software protection and anti-tamper systems. The goal of this topic is to maintain mission assurance and the protection of the critical intellectual property in the event a subset of the system is exploited (e.g., due to supply chain compromise).

Desired architectural attributes of the protection system include, but are not limited to, dynamic/maneuverable protections that force the adversary to exploit a moving target; systems that distributed/fractionate [3] the critical information being protected and force the adversary to attack multiple nodes simultaneously to avoid attack mitigation; redundant systems that maintain mission assurance even in the presence of a subset of compromised and exploited end-nodes; heterogeneous systems that force the development of multiple attack delivery methods and payloads; metamorphism that changes the perceived operational environment and targeted vulnerabilities, and disruptive techniques that break command and control of malicious agents to prevent exploitation.

PHASE I: 1) Design and architect a software protection system containing one or more of the above-mentioned attributes. Development of a minimal prototype to demonstrate feasibility would be beneficial, but is not required provided sufficient design documentation is made available. 2) Develop metrics and a strategy for measuring the effectiveness of the proposed approach. 3) Produce a detailed research report outlining the design and architecture of the system, as well as the advantages and disadvantages of the proposed approach.

PHASE II: 1) Based on the results from Phase I, design and implement a fully functioning prototype solution. 2) Provide test and evaluation results that demonstrate the effectiveness of the overall system. 3) Develop a final report completely describing the design and architecture.

PHASE III DUAL-USE APPLICATIONS: The technology developed under this research topic will maintain mission assurance in the presence of compromised end-nodes and exploited subsystems. DoD applications that will benefit from this technology include a wide range of embedded, sensor, navigation, avionics, and communication systems. Commercial applications include financial, communication, and SCADA systems. As a result, this technology is vital for both the DoD and commercial organizations.

REFERENCES:

[1] The Three Tenets of Cyber Security, http://spi.dod.mil/tenets.htm

[2] Iain Sutherland, Gareth Davies, and Andrew Blyth, "Malware and steganography in hard disk firmware," Journal of Computer Virology, DOI 10.1007/s11416-010-0149-x, http://www.springerlink.com/content/d64241r80qk50824/

[3] United States Air Force Chief Scientist, "Report on Technology Horizons: A Vision for Air Force Science & Technology during 2010-2030"
http://www.aviationweek.com/media/pdf/Check6/USAF_Technology_Horizons_report.pdf

KEYWORDS: Anti-exploitation, cyber maneuverability, distributed systems, fractionated systems, attack disruption

OSD11-IA2 TITLE: Software Deception as a Countermeasure to Attacks on Software Protection Systems

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop innovative countermeasures to attacks on critical software using software decoys and deception.

DESCRIPTION: The effective use of deception in traditional warfare dates back thousands of years [1]. Most notably, its effective use has been demonstrated in World War II [2] and Operation Desert Storm [1]. However, research on the use of software decoys and deception, as a defensive mechanism in software protection systems is currently limited. There are a number of possible reasons for this. First, deceptive techniques do not (by themselves) provide secure systems, since they often are dependent on the mindset of the adversary, which is either not known or not well modeled. Secondly, deception techniques are often viewed as 'single use' technology, since once the deception is exposed that particular deceptive technique can no longer be used in the same scenario. Third, software decoys often cannot be generalized and require tailoring by subject matter experts to make them indistinguishable from the legitimate applications that are the target of attack. Software deception [3] has, therefore, become a highly underutilized tactic in an overall strategy to defeat cyber attacks by providing a layered defense.

To remedy the disadvantages noted above, we desire to develop a software deception strategy and architecture, with techniques that can measurably increase the effectiveness of software protection systems with statistical significance. This topic will contribute to an overall plan to understand the adversary's strategies and tactics in order to build real-time adaptive software protection systems. Components to the plan include inferring adversarial intent to determine the purpose of the attack; extracting adversarial reasoning to determine our opponents goals and strategy in order to predict their 'next move', and the use of deception for tactical advantages, including attack misdirection and avoidance. Research areas of interest include, but are not limited to, the use of deception for (1) adversarial intent (2) adversarial reasoning [4], (3) attacker attribution, (4) attack avoidance/delay, and (5) intelligence gathering.

PHASE I: 1) Develop a strategy and architecture using software decoys and deception as a countermeasure to attacks on critical software and data. 2) Develop a concept for building individual software decoys and deceptive techniques that will plug into the overall system, and design one or more individual decoys or deceptive techniques, 3) Develop metrics and a strategy for measuring the effectiveness of the proposed decoys and/or deceptive techniques. 4) Produce a detailed research report outlining the design and architecture of the system, as well as the advantages and disadvantages of the proposed approach.

PHASE II: 1) Based on the results from Phase I, design and implement a fully functioning prototype solution. 2) Provide test and evaluation results that demonstrate the effectiveness of individual software deception techniques and decoys, as well as the effectiveness of the overall system 3) Develop a final report describing the strategy, architecture, and the design and development of individual decoys or deceptive techniques.

PHASE III DUAL-USE APPLICATIONS: The technology developed under this research topic will mitigate the risk of attack on software protection systems and lead to mission assurance. DoD applications that will benefit from this technology include a wide range of embedded systems, such as weapons systems, avionics, communications, and sensor systems. Commercial applications include insider threat attribution, communication systems, SCADA systems, and other high-value targets, such as banking systems. As a result, this technology is vital for both the DoD and commercial organizations.

REFERENCES:

[1] Jon Latimer, "Deception in War," The Overlook Press, New York, 2001.

[2] Ewen Montagu, “The Man Who Never Was,” Oxford University Press, New York, 1996.

[3] Edward Waltz and Michael Bennett, “Counterdeception Principles and Applications for National Security,” Artech House Publishers, February 2007.

[4] Alexander Kott and William M. McEneaney, “Adversarial Reasoning: Computational Approaches to Reading the Opponents Mind.”

KEYWORDS: Software Decoys, Software Deception, Adversarial Reasoning, Software Protection

OSD11-IA3 TITLE: Identification of Critical Resources and Cyber Threats in the Physical Domain

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: The focus of this research is to develop an innovative system that assists users in rapidly identifying and mapping cyberspace and physical infrastructure to analyze critical threats and vulnerabilities that impact both DOD force projection and mission assurance.

DESCRIPTION: Cyber attacks have become a significant threat for DoD operations that are increasingly more connected and integrated. As DoD relies more on commercial support for communication, troop movement, bases logistical infrastructure support, the threat to those operations from a cyber warfare perspective increases. Much research has been performed to date; however there is a strong need for technologies that automatically discover and correlate physical threats to or critical centralization of cyber resources. Current cyber and network defense is too focused on virtual resources alone. Almost all cyber defense is performed “on the network” ignoring other critical factors. These methods often ignore threats in the physical (kinetic) domain. Importantly, these threats can go both ways. For example, a physical threat to a military installation can map to a particular threat source, but cyber threats can map to multiple communication nodes across multiple DoD networks without geographic constraints. Proposed solutions should allow users to easily provide mappings, automatically identify as many mappings as possible, and provide mechanisms to incorporate new discovery schemes. Furthermore, the solution should help users quickly identify single-points of failure and to measure criticality of components. Commercial, government, DoD, and ad-hoc networks have become nearly ubiquitous. Through extensive abstraction, heterogeneous systems interconnect and interoperate. Unfortunately, these abstractions make system characterization difficult at best. For example, an organization may lease network resources from two different providers for redundancy. These networks may be carried on a single fiber, owned by a common single carrier further upstream. For example, long-haul fiber and Dense Wavelength Division Multiplexing (DWDM) network increase the likelihood that multiple carriers share physical infrastructure. Further, off-network infrastructure requirements such as power, cooling, and maintenance complicate an assessment. The focus of this research is threefold. First involves the development of a methodology for gathering the critical cyberspace and physical data. Second, it involves the development of algorithms, tools, and techniques to automatically generate mappings of virtual to physical resources, and to isolate critical components. The third is the development of a modular operations visualization and analysis framework. New technologies are needed to gather data, assess vulnerabilities, identify critical dependencies and develop capabilities to help in understanding the 1st, 2nd, and 3rd order of effects to DOD when critical infrastructure like power plants, air traffic control systems, sensor webs, and the electrical grid do not perform correctly. The new framework should allow for quick integration of data sources, provide intuitive visualization (such as a geo-located threats on a world map), and allow users to manually map between the cyber and physical domains to support decision aiding and assessment. The framework and these data should be structured such that future components can analyze the multi-domain model for effective and innovative operations.

PHASE I: Develop a design that will acquire, store, map, and visualize information linking cyber and physical resources in a coherent operational picture. Technical work should focus on reducing risk for future phases and developing key technologies to facilitate future work. Special attention should be paid to gathering the data, to identifying potentially complex mappings and identifying gaps. Phase I will include a proof of feasibility of key enabling technologies.

PHASE II: Develop prototype software that can be accredited at Technical Readiness Level 6 (TRL 6), that will effectively acquire, store, manipulate and present the cyber threat and infrastructure data. Create an effective demonstration that uses representative data to provide proof of concept for computer network defense systems that defend against emerging threats.

PHASE III -- DUAL-USE COMMERCIALIZATION: Military Application: Military operations through cyber attacks and the ability to quickly and efficiently identify threats and vulnerability to infrastructure as they relate to cyber assets. Commercial Application: The monitoring, identification, and reconstitution of cyber threats is a critical component of overall readiness and infrastructure information to both the planners and first responders.

REFERENCES:
1. A. Bargar, "DoD Global Information Grid Mission Assurance", CrossTalk: The Journal of Defense Software Engineering, July 2008, http://www.stsc.hill.af.mil/crossTalk/2008/07/0807Bargar.html

2. "Information Assurance (IA) Implementation", DoDI 8500.2, February 6, 2003, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.

3. SCADA, Wikipedia, http://en.wikipedia.org/wiki/SCADA.

KEYWORDS: Cyber threats, networking, mission assurance, operation through cyber attack, information assurance, computer network defense (CND), supervisory control and data acquisition (SCADA)

OSD11-IA4 TITLE: Cyber Security High Abstraction Contextual Visualization and Decision Support System

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop dynamically adjustable trustworthiness metrics that are tuned to human relevance and to automated protocols and that can be manipulated with a highly abstract, tangible interface.

DESCRIPTION: During a cyber attack, Continuity of Operations, or other high-rate dynamic context shift of events, trustworthiness metrics can be so dynamic that cyberspace operators need a real-time high-abstraction interface that enables on-the-fly control of autonomic systems. Allowing users to control the scope of what they believe is currently relevant may help enable autonomic and net-centric system of systems to aid the operation of highly volatile situations encountered during net-enabled spectrum warfare.

Cyberspace analysts must monitor vast amounts of information to enable secure and effective operations. There are human and automated protocols in place to support this activity, but the subsequent presentation of this information is not optimized. Therefore, the intent of this research is to develop a simple-looking visualization and control system that semi-automatically adjusts to events of relevance in the cyberspace domain in an intuitive way to provide only the appropriate trustworthiness metrics needed for the human supervision of the autonomic trust protocols.

By allowing very high abstraction control of the top four to seven (+/- 2) things that users care most about at the moment of use (see citations 5 & 6 below), the system could re-orient the display based on the dynamic scope control of an underlying ontology representing the breadth of many possible trustworthiness measures that may be of interest at different phases of sensor system of system operation and context of use. By allowing the system to dynamically choose scope using abstract representations like topic maps (see 1 below), the appropriate trustworthiness metrics would be presented to the user and subsequent demand for that kind of data passed to relevant cyberspace systems for cyber protocol tasking and refinement of data fusion and data analysis.

With the convergence of several streams of technology and with new understanding from the social sciences, a new capability has emerged in the visualization and control of cyber security systems. Protocols for maintaining operator trust are based on trustworthiness metrics of the underlying computer and communication systems that are context dependent. Some protocols may be more efficaciously invoked than others depending on the situation. Which protocols the system invokes may be determined before hand by the weightings and priorities of decision support algorithms, but those traditional artificial intelligence and machine learning approaches have yet to enable fully automated control of sophisticated protocols across the vast array of possible situations that may arise. Therefore, a mixed initiative human-machine system is required that blends initiative taken by human operators with their automated systems.

Mixed-initiative control is premised on functional abstraction hierarchy representations that look like a work-breakdown structure of activity from strategic level objectives down to actual protocol invocation by automated systems. Adjustment of the displayed level of abstraction requires a dynamic representation of the context to know what is most important for the user to see at any given moment. The traditional means of addressing visualization and control of trustworthiness metrics have been tried and found wanting (4 & 7), and are therefore excluded from this call for proposals unless they include novel application of emerging technologies. One such possibility has emerged from the convergence of three schools of diverse disciplines of Topic Maps, Tangible Interfaces and Sandplay Therapy. (1, 2 & 3) This convergence may be further aided by the advance in electronic location technologies such as RFID. A final enabler of this convergence is the growing youth culture of gaming. Combining gaming culture's use of tangible and computer displays with the social, psychological and computer interface technologies could be a convergence that allows for a long sought advance in high abstraction interfaces that control other displays, algorithms and devices while being tightly synchronized with the current situation and context of use for easy manipulation by a user. Thus, proposals are being sought that offer any effective set of novel combinations of new and emerging interdisciplinary technologies while excluding solutions that offer single discipline, traditional approaches.

The goal of this topic is to conduct new and innovative, interdisciplinary research and development in technologies for selecting appropriate trustworthiness protocols using advanced human/machine interfaces for the visualization and control in a cyberspace security contexts of use.

PHASE I: Phase I activity shall include: Design and develop new visualization and control interface technologies that finds the relevant subset of trust measures and uses these to adjust context dependent trustworthiness metrics, which will thus enable semi-automated use of trust maintenance protocols and demonstrate a proof-of-principle prototype for a cyberspace security scenario that shows the control of high abstraction representations and their linkage to underlying trustworthiness metrics.

PHASE II: The researcher shall develop and demonstrate a comprehensive prototype implementing the Phase I technologies to show ability for extending this to many relevant trustworthiness metrics for cyberspace use cases with several realistic trust protocols and demonstrating a high abstraction representation and interface controlling automated trust maintenance protocols. The researcher shall detail the Phase III plan.

PHASE III -- DUAL USE COMMERCIALIZATION:
Military application: The desired product for cyber security applied to Command, Control, Intelligence, Surveillance and Reconnaissance (C2ISR), Electronic Warfare Battle Management or sensor resource management.
Commercial application: This system would benefit any commercial application dealing with gaming and psychology research or psychotherapy instrumentation or analysis.

REFERENCES:

1. The XML Topic Maps (XTM) syntax created by the TopicMaps.Org consortium is now also included as a normative appendix to the Second Edition of the ISO standard (ISO 13250:2002) along with an interchange syntax which uses SGML. [http://www.techquila.com/topicmaps.html]

2. Brygg Ullmer and Hiroshi Ishii, Emerging Frameworks for Tangible User Interfaces in "Human-Computer Interaction in the New Millenium," John M. Carroll, ed.; © Addison-Wesley, August 2001, pp. 579-601.

3. Barbara A Turner, Handbook of Sandplay Therapy, Temenos Press, Cloverdale, California, 2005

4. Conti, G. (2007). Security Data Visualization: Graphical Techniques for Network Analysis. San Francisco: No Starch Press.

5. Simons, D. J. (2000). Attentional capture and inattentional blindness. Trends in Cognitive Science, Vol. 4, Num. 4, pp. 147-155.

6. Cowan, N. (2000). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. Behavioral and Brain Sciences 24, 87-185.

7. Few, S. (2006). Information Dashboard Design: The Effective Visual Communication of Data. Sebastopol, CA: O'Reilly Media.

KEYWORDS: Trustworthiness metrics, Cyber security, Context, Topic maps, Ontologies, Tangible Interfaces, Gaming Technologies, Psychology protocols, Sandplay psychotherapy, Information Dashboards, RFID, Information Dashboard, Attention, Functional Abstraction Hierarchy

OSD11-IA5 TITLE: Deterministic Detection for Hijacked Program Execution

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: The objective of this SBIR topic is to design and develop a method for reliable and deterministic detection method for hijacked execution (D2HE), and to evaluate its capability, performance, and cost.

DESCRIPTION: Achieving information dominance requires Department of Defense (DoD) to provide information assurance within its information infrastructures. COTS based hardware and software in our computing systems and the network are large, complex and hence inherently insecure. Malwares and adversaries regularly exploit our inherently insecure computing infrastructure. Many approaches have been used to detect malwares and adversarial intrusion activities. The approach varies from detecting the malware signatures, heuristics behavior monitoring, white-listing, marking data entering the system (taint tracking), etc. However, even with all of these security mechanisms, malwares and adversaries still manage to penetrate our system.

One of the often used detection approaches is to insert checkpoints or assertions into the body of the program via code rewriting process. The location of the check points can be derived from code-analysis or from formal model of the program. This approach can be effective in detecting error and improper state in a program. An issue with this approach, in an adversarial situation, is that if the execution of the program is maliciously diverted by an adversary (or malware), the subsequent checkpoint may never be reached, and the execution flow diversion may never raise any alarm.

It is desirable to have a reliable and deterministic alarm which will always ring every time a program is hijacked. The word reliable indicates that the alarm cannot be circumvented and deterministic means that the detection mechanism is has 0% false positive (not statistical or probabilistic). Furthermore, it can be observed that a simple mechanism operating on one or small number of invariants, as oppose to complex state/rule-based system operating on multiple events/sequence of events, such as behavior based detection [3][4][5], may be advantageous for achieving 0% false positive while minimizing false negatives. An example of a deterministic method for recognizing hijacked execution is the venerable taint-tracking method [1][2]. An invariant in this case is a physical and/or logical condition which always occurs during execution hijacking, for example, an external data/string being executed during execution hijacking is the invariant used in the taint tracking methods [1][2].

Understanding of the invariants in an execution hijacking process plays important roles in deterministically recognizing it. The challenge in this topic is to develop a reliable and deterministic detection method for hijacked execution, making use of one or small number of the invariant properties of the execution hijacking process.

PHSE I: Design and develop an efficient method for a reliable and deterministic detection method for hijacked execution flow (D2HE). Develop a proof of concept prototype for D2HE in an open-source OS environment, and investigate its cost and effectiveness.

PHASE II: Further develop and mature D2HE method, develop a full scale D2HE protected system, and perform full-scale evaluation on the system.

PHASE III Dual Use Application: This system could be used in a broad range of information security products within the military, as well as in civilian enterprise applications. The technologies developed in this SBIR will be beneficial in providing additional resiliency to networked enterprise computing system against malwares and intrusions.

REFERENCES:

1. J. Newsom, D. Song, “Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software”, Proceedings of IEEE Symposium on Security and privacy 2005.

2. G.E. Suh, J.W. Lee, D. Zang, S. Devadas, “Secure program execution via dynamic information flow tracking”, Proceedings of International Conference on Architectural Support for Programming languages and Operating Systems 2004.

3. R. Sekar, M. Bendre, D. Dhurjati, P. Bollineni, “A fast automaton-based method for detecting anomalous program behaviors”, Proceedings of IEEE Symposium on Security and privacy 2001.

4. M. Sharif, W. Lee, W. Chui, A. Lanzi, “Secure in-VM monitoring using hardware virtualization”, Proceedings of ACM conference on Computer and Communication Security 2009.

5. S. Fischmeister, Y. Ba, “Sampling-based Program Execution Monitoring”, Proc. of the ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES) 2010

KEYWORDS: Execution flow hijacking, malware detection, intrusion detection, program flow tracking, information flow tracking, deterministic detection

OSD11-IA6 TITLE: Active Software Defense to Reduce Threat Capability Effectiveness

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop innovative software protection technology containing the ability to support the active defense of critical software applications.

DESCRIPTION: Current software application defenses are largely passive in nature [1]. When an attack is detected, these defenses often impose indirect penalties (e.g., deleting cryptographic keys or zeroing memory) in such a manner that it forces the adversary to reacquire the software and hardware assets, but impose no real-time penalties on the attacker that prevent the application from becoming compromised in the first place [2] [3].

The focus of this topic is to develop intelligent and cooperative software protection agents that can deploy active defensive countermeasures [4] and be used in conjunction with other forms of software protection. The desired software protection system should meet the following requirements: (1) have the ability to monitor, in real-time, protected end-nodes and report suspicious activity indicating a possible attack; (2) have the ability to gather forensic information on the protected host related to the attack; (3) have the ability to synthesize and assess the collected information to form a response to an attack; and (4) have the ability to impose direct penalties on the attacker within the boundaries of the protected host or network environment.

The software protection solution should contain the ability to perform surveillance as well as protection, and should have the ability to discriminate between a legitimate user and an attacker. Using the captured surveillance information, the solution should have the ability to react to an attack (e.g., terminating the network connection, stopping malicious processes, or denying the use of attack tools). Surveillance information of interest includes, but is not limited to, knowledge of the attacker’s behavior, attack tools and methods used, the type of information being sought in the attack, and the origin of attack. In the absence of connectivity with human operators, the active defensive system must have the ability to act autonomously and respond to an attack, contingent upon meeting pre-determined criteria. Proportional and subtle responses to an attack are important elements in the protection scheme. Responses must only occur once it is determined with a high degree of certainty that the host or network the application resides on is under attack or has been compromised, and the proposal should specify a policy for when such penalties will be invoked and with what severity.

An example of a system employing active defense is a protection system that (upon attack detection) can intelligently and proportionally respond to the attack, including sending a warning to a system administrator for a benign policy violation, redirecting an attacker to a honeypot for intelligence gathering, terminating a network connection, or covertly degrading the target application prior to piracy by the adversary.

PHASE I:
1) Research and develop a concept for an active software defense that meets the above mentioned requirements. Operating systems of interest include Linux or Windows.
2) Provide design and architecture documents of a prototype tool that demonstrates the feasibility of the concept.
3) Provide a minimal software prototype that meets one or more of the four requirements listed above.

PHASE II:
1) Based on the results from Phase I, refine and extend the design of the active software defensive system prototype to a fully functioning solution.
2) Provide test and evaluation results demonstrating the ability of the prototype to deploy active countermeasures on attackers.

PHASE III DUAL-USE APPLICATION: Active software defensive technology will serve to protect critical intellectual property by preventing attacks in real-time, gathering forensic evidence concerning the attack, or invoking a penalty on the attacker; and as such will find application in both the government and commercial sectors. Commercial applications can use the active defensive software protection technology described above to monitor, control, debug, configure, authenticate, update, and patch critical software and data with a reduced risk of exploitation [5]. Enterprise software that has embedded situational awareness can be used to authenticate and ensure trust in end-node applications.

REFERENCES:
[1] Dr. Mikhail J. Atallah, Eric D. Bryant, and Dr. Martin R. Stytz, “A Survey of Anti-Tamper Technologies,” CrossTalk: The Journal of Defense Software Engineering, November, 2004, http://www.stsc.hill.af.mil/crossTalk/11/0411Atallah.pdf

[2] Wm. A. Wulf, “Cyber Security: Beyond the Maginot Line,” Presented before the House Science Committee, U.S. House of Representatives, Oct 10, 2001, http://www.nae.edu/nae/naehome.nsf/weblinks/MKEZ-542KBP?OpenDocument

[3] Cyber officials: Chinese hackers attack ‘anything and everything’ http://www.fcw.com/article97658-02-13-07-Web&printLayout, Feb. 13, 2007.

[4] Laurent OUDOT, Digital Active Self-defense, http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-oudot-up.pdf, 2004.

[5] Check Point Introduces New Active Defense Security Category: Unveils SmartDefense for Advanced, Real-Time Protection Against All Types of Network Attack, http://www.checkpoint.com/press/2002/smartdefense042502.html

KEYWORDS: Software Protection, Software Agents, Covert Communications, Software Countermeasures, Situational Awareness, Active Defense